Unit IV

CHAPTER 4

Security Requirements

Syllabus

IP Security : Introduction, Architecture, IPV6, IPv4, IPSec protocols, and Operations, AH Protocol, ESP Protocol, ISAKMP Protocol, Oakley determination Protocol, VPN. WEB Security : Introduction, Secure Socket Layer (SSL), SSL Session and Connection, SSL Record Protocol, Change Cipher Spec Protocol, Alert Protocol, Handshake Protocol. Electronic Mail Security : Introduction, Pretty Good Privacy, MIME, S/MIME, Comparison. Secure Electronic Transaction (SET).

Syllabus Topic : Security Introduction

4.1 IP Security - IP Security Overview

→ **(SPPU - May 15)**

Q. 4.1.1 Define IP sec. (Ref. Sec. 4.1) May 15. 2 Marks

Q. 4.1.2 What is IPSec? (Ref. Sec. 4.1)

- The network connectivity not only gives us authority to access world from computer but at the same time the network lets the outer world access to us in the way that we may not be desire. Any loop hole in our network can make our systems vulnerable and we can be the victim of cybercrime.
- To secure information and to send data through network are both linked to each other. One formal way that network engineer's uses for data communication is the OSI seven layer model for networking.
- The OSI model describes the seven layers of interaction for a system communication in the network.
- Starting from the top most layer data is sent to layer by layer, each layer adding its own information to the original information until the original data and the added content of each layer reach to the physical medium.
- All the layers "communicate" with each other at the sender and receiver side, they need to send pure data and data should be intact with no change at the receiver's side. Reviewing the flow of information through the layers, we observe that all layers depend upon each other so security is important in each layer.
- The OSI security architecture reference model (ISO 7498-2) is designed around the seven layers of OSI reference model (ISO-7498-1), reflecting the different requirements of security in each layer for secure data transfer.
- In TCP/IP protocol suite there are various protocols and techniques used to secure data and ongoing traffic at each layer called as layer wise security concerns. At the network (internet) layer TCP/ IP supports the most significant protocol called Internetworking Protocol/ Internet Protocol (IP).
- **Internet Protocol security (IPSec)** is a framework of open standards for protecting communications over Internet Protocol (IP) networks through the use of cryptographic security services. The most important feature of IPsec is that it can authenticate and encrypt all on-going traffic at the IP level.
- In terms of cryptography Internet Protocol support for sending and receiving encrypted information of any kind without any modification. IPSec provides different kinds of cryptographic services like confidentiality integrity and authentication.
- Table 4.1.1 shows the layers and the perspective security in each layer.

Table 4.1.1

Layers (ISO 7498-1)	ISO 7498-2 Security Model
Application	Authentication
Presentation	Access Control
Session	Non-Repudiation
Transport	Data Integrity
Network	Confidentiality
Data Link	Assurance / Availability
Physical	Notarization / Signature

Syllabus Topic : Architecture

4.2 IP Security Architecture

Q. 4.2.1 Distinguish between tunnel and transport mode in IPSec. Describe briefly how IPSec work. (Ref. Sec. 4.2)

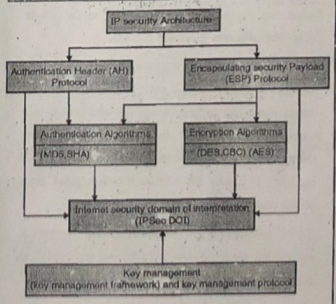

Fig. 4.2.1 : IPSec architecture

- IPSec was designed by the Internet Engineering task force IETF. It is a collection of protocols which provides security for a packet at network level. IPSec creates authenticated and confidential packets for network layer also known as IP (Internet protocol layer).
- IPSec provides node to node communication in routing protocols; it provides security to other protocols also which are used for client-server communication in transport layer.
- IPSec defines two protocols as they are backbone of IPSec, are Authentication Header (AH) and Encapsulating Security Payload (ESP) protocol. Architecture of IPSec is shown in Fig. 4.2.1 and following sections defines details on each fields.

1. Authentication Header (AH)

It defines the AH packet format for processing incoming and outgoing packets. AH helps to ensures that authentication and integrity of the data/packets is protected.

2. Encapsulating Security Payload (ESP)

It defines the ESP packet header, which transmits packets in encrypted and unreadable format. ESP helps to ensure that confidentiality, authenticity and integrity of the data is protected.

3. Authentication Algorithms

Use of MD-5 and SHA with Encapsulating Security Payload and Authentication to achieve integrity and protection of data. Hash is attached to the IP header as an integrity checksum.

4. Encryption Algorithms

Few standard encryption algorithms are implemented in IPSec are DES, AES and CBC because of large key size to secure data.

5. Internet security Domain of Interpretation (DOI)

It contains the supporting database of all IP Security protocols, their parameters, all defined algorithms, key size with lifetime and identity of all approved encryption and decryption algorithms.

6. Key Management

As defined earlier key management is used to generate and distribute the keys required for IPSec protocols.

4.2.1 IPSec Modes

IPSec operates in two different modes :

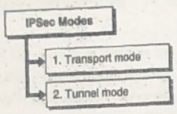

Fig. 4.2.2 : IPSec Modes

1. Transport Mode

- In Transport mode IPSec protects the data that is delivered from transport layer to network layer or in other words we can say that, transport mode protects the payload(a packet consist of controlled information and user data) of network layer.
- It encapsulates the transport layer payload by adding IPSec header and IPSec trailer and sends this encapsulated packet to network layer.
- After that the IP header of network layer is added to that encapsulated payload. IPSec transport mode is responsible for complete delivery of packet (traffic) from one host to another host or from host to gateways called as end-to-end communications.
- End-to-End communications means communications between client machine and a server machine, communications between two routes and from router to gateway is also considered as end-to-end communication. IPSec transport mode is responsible for secure communications between all these devices.
- Transport mode helps to protect user data, also known as IP payload through an AH or ESP header. In transport mode payload of IP packet is encrypted by the IPSec headers and trailers but the IP header information, which is remain unchanged. The payload of an IP packet is protected before it is handled by the network layer as shown in as in Fig. 4.2.3.
- Fig. 4.2.4 shows how the data exchange (end to end security) take place after encrypting payload.

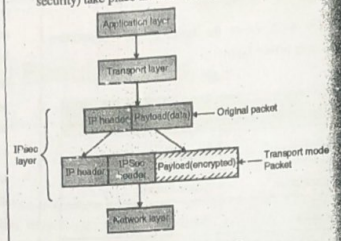

Fig. 4.2.3 : Transport mode

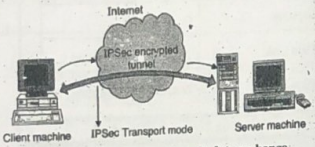

Fig. 4.2.4 : IPSec Transport mode data exchange

2. Tunnel Mode

- In tunnel mode the IPSec protects the entire IP Packet of Network Layer.
- It takes whole IP packet including the header of that IP Packet and applies the IPSec method to the whole packet and adds new IP header.
- IPSec tunnel mode is responsible for network-to-network communications, it encrypt the traffic between routers, gateways or host-to-network and host-to-host communications over the Internet and creates a secure tunnel. IPSec tunnel mode encrypts complete IP packet including IP header and transfer it over network layer (entire original IP packet is encrypted).
- Tunnel mode binds the original IP packet, encrypts it, adds a new IP header and IPSec header and sends it to the other end of IPSec shown in Fig. 4.2.5.
- Fig. 4.2.6 shows IPSec tunnel mode during data exchange process.

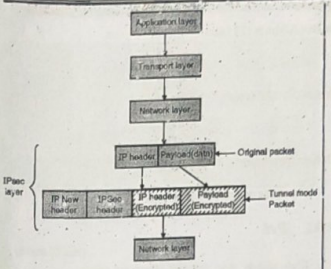

Fig. 4.2.5 : Tunnel Mode

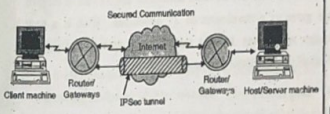

Fig. 4.2.6 : IPSec tunnel mode data exchange

- Tunnel mode is used on most of the IPSec gateway devices such as firewalls, routers, and connecting remote locations such as branch offices, organizations, and universities securely through a network called Virtual Private Network (VPN).
- The entire original, inner, packet travels through a tunnel from one point of an IP network to another;
- Tunnel mode is generally used for secure communication between two routers, a host and a router or vice versa.

Syllabus Topic : IPv6 and IPv4

4.3 IPv6 and IPv4

→ (SPPU - May 15)

Q. 4.3.1 Discuss IP sec protocols in detail. (Ref. Sec. 4.3) **May 15, 6 Marks**

Before discussing IPv6 first we need to understand basics of IPv4.

4.3.1 IPv4

IPv4 is a Network Layer Protocol. IPv4 Stands for Internet Protocol Version 4. An IPv4 address is a 32-bit :

- Address that uniquely identifies host or a computer to the Internet.
- Length of IPv4 address is a 32-bit IPv4 Address are unique and all nodes connecting Internet must have IPv4. The address space of IPv4 is 2^{32} or 4,294,967,296.
- Dotted decimal notation of IPv4 is representing as 192.168.0.1 (each single byte separated. (dot) symbol)
- Packets in the network layer is called as datagram's, which consist of two parts : header and data. The header is 20 to 60 bytes in length and contains necessary information about delivery of the packet from one router to another as shown in Fig. 4.3.1.

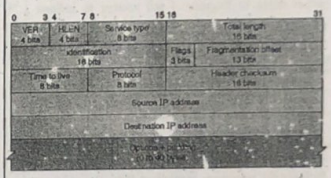

Fig. 4.3.1 : IPv4 Packet Format

- Detail explanation about of each field is given below.

Version (4 bits)

Indicates the version of IP and is set to 4.

Internet Header Length (4 bits)

- Indicates the number of 4-byte blocks in the IPv4 header (Length of entire IP header).
- Because an IPv4 header is a minimum of 20 bytes in size, the smallest value of the Internet Header Length (IHL) field is 5.

Type of Service (8 bits)

Indicates the desired service expected by this packet for delivery through routers across the IPv4 internetwork.

Total Length (16 bits)

Indicates the total length of the IPv4 packet (IPv4 header + IPv4 payload) that is up to 65,535 bytes long

Identification (16 bits)

- Identifies this specific IPv4 packet.
- The Identification field is selected by the originating source of the IPv4 packet. If the IPv4 packet is fragmented, all of the fragments retain the
- Identification field value so that the destination node can group the fragments for reassembly.

Flags (3 bits)

- Identifies flags for the fragmentation process.
- There are two flags one to indicate whether the IPv4 packet might be fragmented and another to indicate whether more fragments follow the current fragment.

Fragment Offset (13 bits)

Indicates the position of the fragment relative to the original IPv4 payload.

Time to Live (8 bits)

- Indicate the maximum number of links on which an IPv4 packet can travel before being discarded.
- Therefore, the TTL becomes a maximum link count with the value set by the sending node.

Protocol (8 bits)

- Identifies the upper layer protocol.
- For example, TCP uses a Protocol of 6, UDP uses a Protocol of 17, and ICMP uses a Protocol of 1.

Header Checksum (16 Bits)

- Provides a checksum on the IPv4 header only.
- Each IPv4 node that receives IPv4 packets verifies the IPv4 header checksum and silently discards the IPv4 packet if checksum verification fails. Therefore, the Header Checksum is recomputed at each hop between source and destination.

Source Address (32 bits)

Stores the IPv4 address of the originating host.

Destination Address (32 bits)

Stores the IPv4 address of the destination host.

Options (multiple of 32 bits)

Stores one or more IPv4 options.

4.3.2 IPv6

IPv6 stands for Internet Protocol version 6. As discussed earlier the Internet addresses are 32 bits in length; this gives us a maximum of 2^{32} addresses. IPv6 is a new design which has 128-bit address that give much greater flexibility in address allocation.

☞ **Why IPv6 ?**

- Larger address space
- Better header format
- New options
- Allowance for extension
- Support for resource allocation
- Support for more security
- Support for mobility

☞ **IPv6 address format (128 bits)**

2031:0000:130F:0000:0000:09C0:876A:130B

- 8 groups of 4 hexadecimal digits
- Each group represents 16 bits
- Separator is ":"
- Case-independent
- Leading zeros in a field are optional:
  2031:0:130F:0:0:9C0:876A:130B

☞ **IPv6 Header Format**

Fig. 4.3.2 shows format of IPv6.

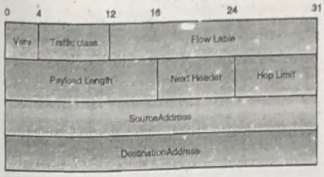

Fig. 4.3.2 : IPv6 Header Format

Version (4 bits)

4 bits are used to indicate the version of IP and is set to 6.

Traffic Class (8 bits)

The 8-bit field in the IPv6 header is available for use by originating nodes and/or forwarding routers to identify and distinguish between different classes or priorities of IPv6 packets.

Flow Label (20 bits)

- Identifies a flow and it is intended to enable the router to identify packets that should be treated in a similar way without the need for deep lookups within those packets.
- This label is used to maintain the sequential flow of the packets belonging to a communication.
- Set by the source and should not be changed by routers along the path to destination.
- The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information. This field helps avoid re-ordering of data packets.
- Unique and powerful tool to IPv6.

Payload Length (16 bits)

With the header length fixed at 40 bytes, it is enough to indicate the length of the payload to determine the length of the entire packet.

Next Header (8 bits)

- Indicates either the first extension header (if present) or the protocol in the upper layer (such as TCP, UDP, or ICMPv6).
- When indicating an upper layer protocol above the Internet layer, the same values used in the IPv4 Protocol field are used here.

Hop Limit (8 bits)

In IPv6, the IPv4 TTL was appropriately renamed Hop Limit because it is a variable that is decremented at each hop, and it does not have a temporal dimension.

Source IPv6 Address (128 bits)

Stores the IPv6 address of the originating host.

Destination IPv6 Address (128 bits)

Stores the IPv6 address of the current destination host.

Syllabus Topic : IPSec Protocols and Operations, AH Protocol, ESP Protocol

4.4 IP Security Protocols

→ **(SPPU - May 16, Dec. 16)**

Q. 4.4.1 How AH and ESP are differs while working under transport and tunnel mode ? (Ref. Sec. 4.4)

Q. 4.4.2 Describe IPSec protocol with its components and security services. (Ref. Sec. 4.4) **May 16, Dec. 16, 8 Marks**

Encryption of data and its authenticity is prime concern for secure communication, to avail this two features, IPSec provides two protocols at network layer :

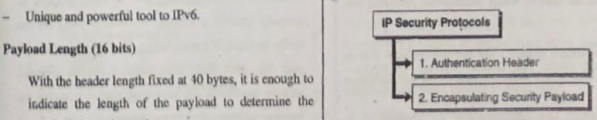

Fig. 4.4.1: IP Security Protocols

4.4.1 Authentication Header

Q. 4.4.3 Explain Authentication Header. (Ref. Sec. 4.4.1)

- It is designed for authentication, integrity of payload which is carried in IP Packet. It is first protocol of IPSec called Authentication Header (AH) protocol designed to provide data authentication (to identify source host), data integrity (if data get modified while in transit) and non-repudiation but doesn't provide data confidentiality (if attacker able to access the contents of a message) because Authentication Header does not encrypt the data/ IP packet.
- The main functionality of this protocol is protection against replay attacks (sending same data to receiver again and again) and protection against tampering of data over a network.
- Authentication Header is also used to protect the upper-layer or the entire IP packet, with the help of message authentication code (MAC - used to generate fixed length value from message and secret key to provide authentication) using well known hashing algorithms like MD5 or SHA1.
- By using Hash function and symmetric key algorithm, message digest is calculated and inserted in authentication data as shown in Fig.4.4.2 because of this AH protocol provides data authentication and data integrity, but not confidentiality or privacy.
- The internal fields of authentication header format are shown in Fig. 4.4.2.
- This protocol uses cryptographic checksum which is similar to hash function or message digest, the checksum is inserted in authentication header and placed in location depends on which mode it is using (tunnel mode or transport mode).

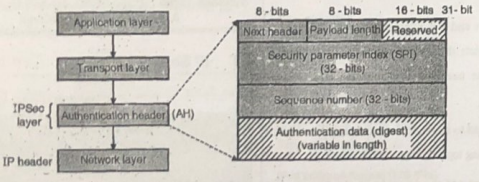

Fig. 4.4.2 : Authentication Header

A brief description of each field

- **Next header (8 bits) :** The next header is an 8 - bit filed which is used to identify the type of payload/ data carried by IP packet.
- Identifies the type of header immediately following this header.
- **Payload length (8 bits) :** The payload header is also an 8 - bit filed which defines length of the authentication header.
- Length of the AH in 32-bit words minus 2.
- **Reserved (16 bits) :** AH contains 16 - bit field which is reserved for future use and always set to zero.
- **Security Parameter Index (SPI) (32 bits) :** SPI is a 32-bit field used in combination with source IP address, destination IP address and AH security protocol to uniquely identify a security association (SA) for the traffic to which IP packet belongs, we will discuss SA it next bit. This field also defining which different security algorithms and keys were used to calculate the message authentication code (MAC).

- **Sequence number (32 bits) :** It is also a 32 bit field. It prevents the retransmission of datagram which is also known as **Replay attack.**
- A monotonically increasing counter value.
- **Authentication Data :** This is variable length field whose length depends upon encryption algorithm used. Authentication data field of AH protocol is the output of hashing algorithm or message digest algorithm. AH protocol performs the Integrity Check Value (ICV) on packet header or MAC is computed over the complete IP packet including the outer IP header to ensure that the data has not been changed during transmission process. As mentioned earlier AH doesn't encrypt the data the reason it doesn't provide confidentiality during transmission.

Modes of Operation

AH can work in two modes :

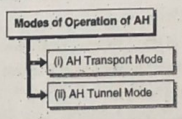

Fig. 4.4.3 : Modes of Operation of AH

(i) AH Transport Mode

In Transport mode the authentication header is placed between original IP Header and original TCP header as shown in Fig. 4.4.4.

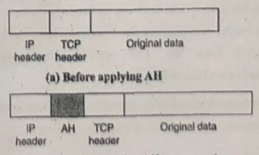

Fig. 4.4.4 : AH transport mode

(ii) AH Tunnel Mode

- In Tunnel Mode the AH is inserted between the new IP header and original IP header.
- The inner IP address contain source and destination address of sender and receiver and the out IP address contain the address of security gateway or firewall as shown in Fig. 4.4.5.

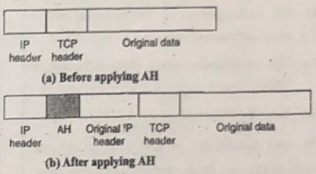

Fig. 4.4.5 : AH tunnel mode

4.4.2 Encapsulating Security Payload

Q. 4.4.5 Explain in detail IPSec ESP format. (Ref. Sec. 4.4.2)

- One of the most important feature that Authentication Header was unable to provide called data confidentiality (if attacker able to access the contents of a message).
- An Encapsulating Security Payload is primarily designed to provide encryption, authentication and confidentiality for the data or payload that is being transferred in an IP network.
- As defined earlier ESP is used to encrypt the entire payload of an IPSec packet the reason ESP alone can provide data authentication, protection against replay attacks and data integrity by adding ESP header, ESP trailer and MAC to the packet.
- ESP has the same fields as defined in AH, but it integrates these fields in a different way instead of having just a header, it divides these fields into three components: An ESP header, ESP trailer and ESP authentication block as shown in Fig. 4.4.6.
- It is designed for confidentiality and integrity of messages. ESP can be used alone or with combination

of AH.ESP adds a header and a trailer to the payload. Following are the steps for adding ESP header and trailer.

Step 1 : In the initial step, ESP trailer is added to IP payload.

Step 2 : Payload and trailer or encrypted

Step 3 : After the encryption ESP header is added to the encrypted packet.

Step 4 : ESP header, payload and ESP trailer are used to create authenticaied data.

Step 5 : This authentication data is added at the End of Trailer.

Step 6 : Lastly the IP header is added.

- The main functionality of ESP is to provide the confidentiality to IP packet by encrypting them. Encryption algorithms (Triple DES, Blowfish, and IDEA etc.)used to combines the data in the packet with a key and transform it into an encrypted form. The encrypted packet now then transmitted to the destination, and decrypts it using the same algorithm.

The detail description of Encapsulating Security Payload (ESP) fields is given below :

- **ESP Header :** This contains two fields, Security Parameter Index (SPI) of 32 bits and Sequence Number of 32 bits, as defined in AH protocol SPI is a 32-bit field used in combination with source IP address, destination IP address and ESP security protocol to identify a security association (SA) for the traffic to which IP packet belongs.
- **Sequence number :** It is also a 32 bit field. It prevents the retransmission of data gram which is also known as **Replay attack as defined earlier.** This field is not encrypted but it's authenticated to perform anti-replay checking before decryption.
- **Encrypted data :** This is variable length filed contains transport layer segment or IP packet which is protected by performing ESP encryption.
- **ESP Trailer :** ESP trailer field contains padding (0-255 bytes), pad length 8- bits and next header 8 - bits.
- **Padding (0-255 bytes) :** Padding filed used to expand plain text message to required size or to align the encrypted data by adding padding bits to the actual data which provides confidentiality to traffic flow.
- If an encryption algorithm requires the plaintext to be a multiple of some number of bytes (e.g., the multiple of a single block for a block cipher), the Padding field is used to expand the plaintext (consisting of the Payload Data, Padding, Pad Length, and Next Header fields) to the required length.
- **Pad Length (8 bits) :** This is mandatory field in ESP protocol which used to indicate the number of pad (protection) bytes added into the packet.
- Indicates the number of pad bytes immediately preceding this field.
- **Next Header (8 bits) :** The same bit length as of pad length used to identifies the type of encrypted data in the Payload Data field.
- Identifies the type of data contained in the Payload Data field (an upper-layer protocol - TCP, UDP, or an IPv6 extension header).
- **ESP Authentication Data :** This is variable length field whose length depends upon encryption algorithm used.
- A variable-length field (must be an integral number of 32-bit words) that contains the Integrity Check Value computed over the ESP packet minus the Authentication Data field.
- As mentioned earlier ESP encrypts the data the reason it provide data confidentialty during transmission.

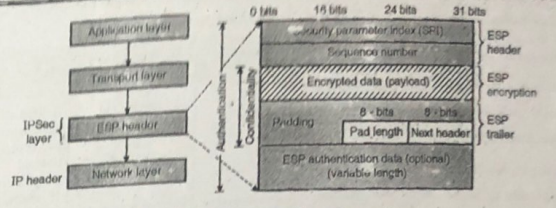

Fig. 4.4.6 : ESP header, trailer and encryption

Modes of Operation

ESP can work in both modes namely :

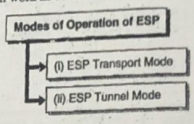

Fig. 4.4.7 : Modes of Operation

(i) ESP Transport mode

In this case ESP header is added before the transport layer header (like TCP,UDP) and trailer is added after the IP Packet whereas if authentication is required then authentication data is added after the ESP trailer. Fig. 4.4.8 shows transport mode in ESP.

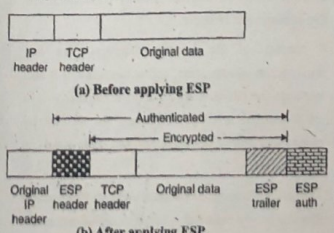

Fig. 4.4.8 : Transport mode in ESP

(ii) ESP tunnel mode

In this case ESP header is added before original IP header and ESP trailer after the original data.

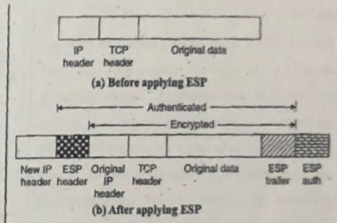

Fig. 4.4.9 : Tunnel mode in ESP

The whole packet is encrypted. As whole packet is encrypted so New IP header will be added, which will contain information for routing from on network to another, so that packet can be transmitted.

Fig. 4.4.9 shows tunnel mode in ESP.

4.4.3 Security Association

- It is an important aspect of IPSec, Security Association (SA) is a contract between the communication parties about factors like IPSec protocol version, mode of operation (tunnel or transport), cryptographic algorithm, key etc. Security Association creates a secure channel between two communicating parties.
- If both AH and ESP are used SA for actual operation then they will need two sets of SA one for AH and one for ESP.
- For communication each party needs two set of SA one for incoming transmission and one for outgoing transmission because SA is simplex unidirectional.

Security Association Database

- Security Association can be very complex.
- Each participating parties need to have inbound and outbound SAs to allow bidirectional communication. It is a two directional table.
- Each row in table defines Security Association which is collectively called as Security Association Database. Each requires party requires maintaining its own database.
- For one way communication (called unidirectional) single SA is required whereas for two way communication (bidirectional) two security association are required. SA uses different parameters to perform data handling between sender and receiver like security parameter index (SPI). IP address of the host (usually destination IP address of end user); encryption algorithms; protocol format (AH or ESP); and security protocol identifier (SPI).
- Almost all these parameters we have discussed in pervious bit still let us have small look out on these parameters.
  - **Security Parameter Index (SPI) :** A 32-bit number used to uniquely identify a particular security association between any connected devices. The SPI is placed in AH or ESP packet for linking the each secure packet to the security association.
  - **Destination IP Address :** Destination IP address of a host, router or firewall who involved in communication or the address of devices for which security associations are established.
  - **Security Protocol Identifier (SPI) :** To identify which protocol (AH or ESP) is used for security associations. If both are used then they have separate security associations.

Tranport vs. Tunnel Mode

Protocols	Transport Mode SA	Tunnel Mode SA
AH	Authenticates IP payload and selected portions of IP header and IPv6 extension headers.	Authenticates entire inner IP packet plus selected portions of outer IP header.
ESP	Encrypts IP payload and any iPv6 extension header	Encrypts inner IP packet
ESP with authentication	Encrypts IP payload and any IPv6 extension header. Authenticates IP payload but no IP header	Encrypts inner IP packet. Authenticates inner IP packet.

Syllabus Topic : ISAKMP Protocol, Oakley Determination Protocol

4.5 ISAKMP Protocol, Oakley Determination Protocol

Q. 4.5.1 Explain Internet key exchange protocol. (Ref. Sec. 4.5)

- ISAKMP stands for Internet Security Association and Key Management Protocol.
- It consists of the security concepts like key management, authorization, and authentication. It also combines the different higher level associations those are established in order to provide the security for government, private organizations, and commercials on the network.
- The Internet Security Association and Key Management Protocol is very essential in order to define procedures and fixing the structure of packets we can say packet formatting which is used to build, negotiate, change/update and delete security associations.
- It also decides the actual properties in terms of payloads for key generation exchange and to do authentication of data.

- The framework involved in this for transferring key and authentication data which is independent of the key generation technique, encryption algorithm and authentication mechanism.
- ISAKMP is totally different from Key exchange protocol. Hence it works as common framework and it can be implemented over any transport protocol.

4.5.1 ISAKMP

→ (SPPU - Dec. 16, May 17)

Q. 4.5.2 Explain ISAKMP protocol for IP sec. (Ref. Sec. 4.5.1) Dec. 16, May 17, 6 Marks

- The internet security association and key management protocol is a framework that defines the formats of payload, the mechanics of implementation of a key exchange protocol, and the exchange of a security association between the parties.
- ISAKMP protocol defines the mechanics of implementing a key exchange protocol, and agreement between communicating parties i.e. which are the different features of IPSec protocol has to use etc. and all (simply its negotiation of security association).

ISAKMP features

- It is used to authenticate of remote entity.
- It manages the secure session between communicating parties by applying different cryptographic techniques.
- Exchanging required information about key sharing.
- Negotiation over all data transmission by applying security policies.
- The reasons ISAKMP establish secure communicating channel between two parties and authenticate them for secure key exchange and negotiation on certain security terms and condition.

ISAKMP header

1. **Initiator cookie** (64 bit) : The cookie of the entity that initiated SA establishment, SA notification, or SA deletion.
2. **Responder cookie (64 bit) :** The cookie of the entity that is responding to an SA establishment request, SA notification, or SA deletion.
3. **Next payload (8 bits) :** Indicates the type of the first payload in the message.
4. **Major version (4 bits) :** The major version of the ISAKMP protocol in use.
5. **Minor version (4 bits) :** The minor version of the ISAKMP protocol in use.
6. **Exchange type (8 bits) :** Indicates the type of exchange being used. This dictates the message and payload orderings in the ISAKMP exchanges.
7. **Flags (8 bits) :** Indicates the options that are set for the ISAKMP exchange.
8. **Message ID (32 bit) :** A unique value used to identify the protocol state during Phase 2 negotiations. It is randomly generated by the initiator of the Phase 2 negotiation.
9. **Length (32 bit) :** The total length of the ISAKMP header and the encapsulated payloads in bytes.

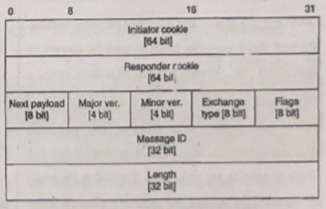

Fig. 4.5.1 : ISAKMP header format

4.5.2 Oakley

→ (SPPU - May 16)

Q. 4.5.3 Explain OAKLEY key determination protocol. (Ref. Sec. 4.5.2) May 16, 6 Marks

- Oakley protocol defines the mechanism of key exchange or key agreement protocols in which two parties must agree on key generated before data transmission.

- IKE uses different cryptographic techniques and security policies for securely exchanging information between two entities such as Diffie-Hellman key exchange, DES, MD5, SHA, RSA algorithm etc.

OAKLEY key determination protocol

- It is a key Determination Protocol proposed by Hilarie K. Orman in 1998, which is a firm base for broadly used Internet Key Exchange protocol.
- Diffie-Hellman key exchange algorithm is used in between authenticated parties', so on insecure connection also both the parties can exchange the keying material over the network. Hence it is also known as Key agreement protocol.
- This protocol was proposed to increase the cryptographic strength where it allows two organizations to agree on a shared value without requiring encryption. The shared value is immediately available for use in encrypting subsequent conversation, e.g. data transmission and/or authentication.
- OAKLEY is a generic key exchange protocol, because the keys that it generates might be used for encrypting data with a long privacy lifetime, 20 years or more.
- For distribution of keys there are some options laid down. Along with Diffie-Hellman key exchange, OAKLEY protocol can be used to generate a new key from an existing key and before distributing the newly (externally) derived key encryption is performed.
- As per the security requirements and performance requirement of two parties protocol allows using some of the forward secrecy features and anti-clogging features. It also gives an authority to use encryption and non-encryption algorithms.

Advantages of OAKLEY key determination protocol

(1) It uses the mechanism of cookie exchange to avoid clogging attacks (DoS type of attack).

(2) It uses nonce (arbitrary number) to detect the replay attacks.

(3) It authenticates the Diffie-Hellman using digital signature, public key encryption or symmetric key encryption to overcome man in the middle attack.

SKEME

It is another protocol for exchanging authenticated key between the parties. It uses public key encryption for authentication in key exchange protocol.

4.5.3 IPSec and IKE (Internet Key Exchange) Relationship

- To protect network from traffic, the SAs are needed to be established in IPSec. If there is no SAs present, the IPSec to protect network from traffic, the SAs are needed to be established in IPSec.
- If there is no SAs present, the IPSec which security parameter will be used for IKE negotiation and protection.
- In the protected session, IPsec SAs are negotiated and established. With a Protection of traffic (IPsec SAs) policy is established and keys are exchanged using the Diffie-Hellman method hence IPsec can start to protect the network traffic. When IPsec SAs' lifetime expires, IKE is invoked again, and new IPsec SAs are created and established.

IKE protocol

When negotiations of IKE begin, it looks for the IKE policy that is same for both the parties. A match is made when both the parties contains same policies for encryption, authentication, hashing and Diffie-Hellman parameter values. If it does not match then IKE refuses negotiation and IPSec SA's will not be established and negotiated for the parties.

4.5.4 IKE Phases and Modes

Q. 4.5.4 Explain different phases of IKE protocol. (Ref. Sec. 4.5.4)

IKE has two phases of operations :

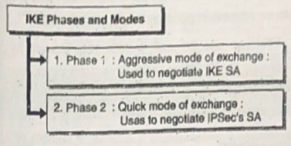

Fig. 4.5.2 : IKE Phases and Modes

→ **1) IKE phase 1 : Aggressive mode of exchange : Uses to negotiate IKE SA**

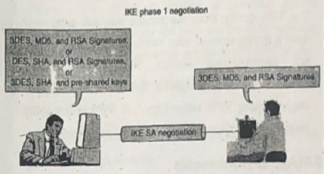

Fig. 4.5.3

For Instance

- As shown in Fig. 4.5.3 user A and user B want to talk IKE, They must agree on a common IKE protection suite.
- The initiator (user A) proposes several protection suites and the responder (user B) chooses one of the offered protection suite.
- The selection is made according to the priorities and the configuration of the responder.
- In the Fig. 4.5.4, user A proposes three protection suites out of which user B chooses the second protection suite. Both must agree on the same protection suite.
- If they do not, no common policies may exist and the IKE session may be terminated.

→ **2) IKE Phase 2 : Quick mode of exchange : Uses to negotiate IPSec's SA**

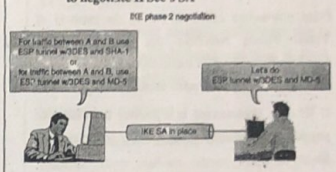

Fig. 4.5.4

For Instance

- As shown in Fig. 4.5.4 user A and user B wish to protect the traffic with IPSec and the IKE SA is already established between them.
- User A proposes various IPSec security policies and user B chooses one of them (with highest priority according to configuration).
- After successful negotiation, keying material is exchanged and IPSec SAs are established to protect network traffic

4.5.5 IP Security Benefits / Applications

→ **(SPPU - Dec. 14)**

Q. 4.5.5 Enlist the applications and benefits of IPSec. (Ref. Sec. 4.5.5)

Q. 4.5.6 What are the benefits of IPSec? (Ref. Sec. 4.5.5) Dec. 14, 4 Marks

- As mentioned earlier IP Sec operates at the network layer where secure data transmission take place. For secure access of remote computer over Internet IPSec is used.
- For securely connecting all branches of bank sectors over internet IPSec protocol is used. For secure communication between same organization which are located at different places.
- For connecting to college server any time from any location IPSec protocol is used.
- Most of the corporate sector allowing employees to performed their task from home and update it to

company server at any time from any location or secure access of company server at any time.

- IPSec now-a-days called as one of the standard of Virtual Private Networks that allow low cost connectivity, secure data transmission between various locations over insecure communication channel.
- If IPSec is implemented in a *firewall or router*, can provide strong security to the ongoing traffic crossing the network.

Syllabus Topic : VPN

4.5.6 VPN

→ **(SPPU - Dec. 16)**

Q. 4.5 What is VPN? Explain types of VPN. (Ref. sec. 4.5.6) **Dec. 16. 6 Marks**

- **VPN stands for Virtual Private Network.** The network technology VPN extends the private network (LAN) over a public network (Internet).
- The computer (or network) can be connected securely using VPN if they are physically connected. The companies use VPN, which allows remote workers to connect securely to their private network over public network.
- Also it is used to interconnect remote offices with a head office. VPN is creating secure tunnel between two more devices. It also helps to protect the web traffic from snooping and interference.

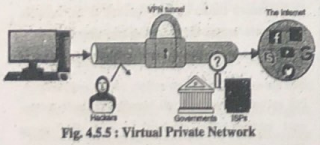

Fig. 4.5.5 : Virtual Private Network

☞ **Advantages**

1. Making client to server connection may not be practical for individual users and also creating WAN connectivity is very costly. VPN is created a secure connection between two endpoints and the information exchanged between the two VPN endpoints is encrypted. So when information is transmitted over the internet no eavesdropping occurs.
2. A VPN can also be used to hide your privacy by disguising true IP address of the user's computer. The company owners protect their identity by using VPN to change their IP address.

☞ **Disadvantages**

1. To encrypt/decrypt and additional data transmission additional processing power required which has have negligible impact on overall usage of the network.
2. The VPN device from one vendor may not work well from a device from another vendor, all VPN devices is not interoperating always. Verify compatibility between the two endpoints by network engineers implementing VPN technology. If VPN is not setup properly then client server connection gets slowdown.

4.5.6(A) VPN Protocols

To create a virtual private network, a virtual tunnel is established between two endpoints via a virtual tunneling protocol or by data encryption. Most popular VPN protocols include IPsec, SSL/TLS, PPTP and L2TP.

1. **PPTP** - The oldest Point-to-point protocol developed by a consortium found by Microsoft, which is supported by vast majority of operating systems. The encryption based on 128-bit key has been cracked, and it is no longer considered very secure
2. **L2TP/IPsec** - VPN based on Layer 2 Tunnel Protocol with IPsec encryption provides more secure service with more features than PPTP.
3. **Open VPN** - Open source technology Open VPN developed on OpenSSL provides secure connection and strong encryption. It has become the default VPN connection type, and is widely supported by 3rd-party software including iOS and Android.

Syllabus Topic : Web Security - Introduction

4.6 Web Security Considerations

→ **(SPPU - Dec. 13)**

Q. 4.6.1 Draw SSL Protocol Stack and explain same. (Ref. Sec. 4.6.1) **Dec. 13. 8 Marks**

The World Wide Web is fundamentally a client/server application running over the Internet and TCP/IP intranets. There are multiple ways or Approaches are used to provides web security.

Most of the ways are similar or provides similar services for the web security but they can be differentiating with the capability and their scope within the TCP/IP stack.

Location of Security facilities in TCP/IP Protocol Stack is shown in Fig. 4.6.1.

- IP security (IPSec) is the one of the important way to provide the web security.
- Advantage of IPSec is that it is transparent to application as well as end user.
- IPSec is used for filtering traffic and it is a general solution for web security.
- Another solution is to implement security just above TCP called as Secure Socket Layer & Transport Layer Security.
- SSL can be embedded in specific packages. For example, Netscape and Microsoft Explorer browsers come equipped with SSL, and most Web servers have implemented the protocol.

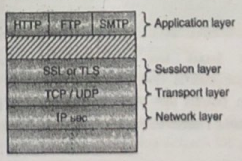

Fig. 4.6.1 : Location of Security facilities in TCP/IP Protocol Stack

☞ **Possible attacks on web security are as follows**

1. **Deceptive phishing**

   Sending bulk of email messages, which make user to click any one of the bulk email such type of attack called as deceptive phishing.

2. **Malware based phishing**

   Running malicious software on target's or users machine. There malware comes from the email attachments.

3. **Key loggers and screen loggers**

   These malware track input from keyboard and send information of target through target's keyboard to hacker (attacker) via internet.

4. **Session hijacking**

   User activities are monitored to get login into the user's system.

5. **Web trojans**

   They are a kind of pop-ups, when logging into some website. These pop ups usually ask for user's credentials.

6. **System reconfiguration attacks**

   It is kind of phishing attack where user's PC setting are modified or changed.

7. **DNS based phishing**

   In this type of phishing the URL requested return to some bogus or fake site which is actually sent by hacker by changing the URL of the requested site of the user.

8. **Content injection phishing**

   It is an act of inserting some malicious content in the websites which can redirect to some other website or may install malware.

9. **Bandwidth attack**

   - Every website is given particular amount of bandwidth to host (e.g. 50 GB) loading of any

websites takes certain amount of time to display whole webpage.

- If more visitors load particular websites page or consumes whole 50 GB bandwidth than particular websites can be ban.
- The attacker does the same by opening 100 pages of site and keeps on loading and refreshing, consuming all bandwidths to make the site out of services.

10. Logic attack

Attack on the network software to make it vulnerable.

For example : in TCP/IP stack.

11. Protocol attacks

This attack, consumes more amount of resources in victims system. It is an attack on the particular features of some protocol that are been installed in the victims systems.

12. Unintentional Dos attack

Sometimes because of huge popularity among users the particular wets suddenly end up.

Solution to achieve web security

- Websites are always to prone to security risks. Website is the main target for installing malicious software or malware on computer. Hackers may also steal important data such as credit card information, destroy the business and can propagate illegal content on user's system.
- **Updated software :** Software updating is mandatory for security consideration.
- **SQL injection :** In SQL injection change in database is done by alerting table data in database.
- **Cross Site Scripting (XSS) :** It allows the attackers to inject client side script into web pages. Therefore, while creating a form it is good to ensure that check the data being submitted and encode or strip out any HTML.
- **Error messages :** While sending error message, it should be prescribed how much information should be send in error message, for example if user is failed while doing logging then user should not come to know which part of login has error username or password.
- **Validation of data :** Both client side and server side data should be valid.
- **Passwords :** It is good to enforce password requirements such as of minimum of eight characters, including upper case, lower case and special character. It will help to protect user's information in long run.
- **Upload files :** The file uploaded by the user may contain a script that when executed on the server opens up your website.
- **SSL :** It is good practice to use SSL protocol while passing personal information between website and web server or database.

Syllabus Topic : SSL, SSL Session and Connection

4.6.1 Secure Socket Layer (SSL)

SPPU - Dec. 14, May 17)

Q. 4.6.2 Explain SSL Protocol interaction sequence diagram between client and server. (Ref. Sec. 4.6.1)

Q. 4.6.3 Discuss SSL with respect to 4 phases.
(a) Establish Security capabilities.
(b) Server authentication and key exchange.
(c) Client authentication and key exchange.
(d) Finish.
(Ref. Sec. 4.6.1)

Q. 4.6.4 Explain architecture of Secure Socket Layer (SSL) (Ref. Sec. 4.6.1) Dec. 14, 8 Marks

Q. 4.6.5 Explain the operation of Secure Socket Layer (SSL) protocol in detail. (Ref. Sec. 4.6.1) May 17, 8 Marks

- Secure Socket layer invented by Netscape communications in 1994. Secure Socket layer is an internet protocol used for securely exchanging the information between client's web browser and the web server.
- Secure socket layer ensure the authentication, data integrity and data confidentiality between web browser and web server i.e. it creates a secure tunnel between

client and server. The main role of SSL is to provide the security to web traffic in all the way.

- The current version of SSL is 3.0. The position of SSL in TCP/ IP protocol suite is shown in Fig. 4.6.2.
- SSL is works in between application layer and transport layer the reason SSL is also called as **Transport Layer Security (TLS).**
- **Transport Layer Security (TLS)** protocol is used to ensure security between communicating applications and their users on the Internet.
- Main function of transport layer protocol is to protect attacker when a server and client communicate, it ensures that attacker or third party should not modify or tamper with any message.
- TLS is the successor to the Secure Sockets Layer (SSL). Will discuss TLS in section 4.6.3.

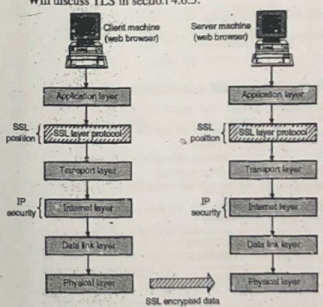

Fig. 4.6.2 : Position of SSL in TCP/ IP protocol suite

- The data will not be passed directly to transport layer instead it will passed to secure socket layer.
- Secure Socket Layer will perform encryption to the data received by application layer and add its own encryption information header called SSH i.e. Secure Socket Layer Header. In the receiver's end SSL will remove the SSH header and then pass data to application layer.
- The Fig. 4.6.2 shows position of SSL protocol in TCP/ IP protocol suite. SSL protocol uses digital certificate and digital signature for securely communication between client machine and server machine.
- SSL encrypt the data received from application layer of client machine and add its own header (SSL Header) into the encrypted data and send encrypted data to the server side.
- Upon receiving encrypted data, server removes the SSL header and decrypts the data and sends the decrypted data to application layer.
- SSL is composed of four protocols in two layers, which support SSL as shown in Fig. 4.6.3. Out of the four, the two most important protocols that are at the heart of SSL are the SSL Handshake Protocol and the SSL Record Protocol, The other two protocols such as SSL Change Cipher Specification and the SSL Alert Protocol play a minor role relatively to previous two protocols.
- The role of these higher-level protocols is the connection establishment, use of required cipher techniques for data encryption and alert (warning, error if any) generation before starting actual data transmission process between client and server.

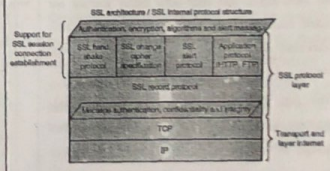

Fig. 4.6.3 : SSL protocols internal architecture

- The SSL Record Protocol is responsible for encrypted data transmission and encapsulation of the data sent by the higher layer protocols (handshake, alert, HTTP) also to provide basic security services to higher layer protocols.

- SSL was designed to make use of TCP protocol to provide a reliable secure process-to-process delivery of entire message/packets.
- We will discuss how client machine securely communicate with the server machine by using underlying network architecture.

4.6.2 Working of SSL

We will discuss SSL Handshake Protocol and the SSL Record Protocol in details.

Syllabus Topic : Handshake Protocol, Change Cipher Spec Protocol

4.6.2(A) Handshake Protocol

➔ **(SPPU - May 15, May 16, Dec. 16)**

Q. 4.6.5 Explain the handshake protocol actions in SSL. (Ref. Sec. 4.6.2(A))

Q. 4.6.6 Explain steps of SSL handshaking protocols. (Ref. Sec. 4.6.2(A)) **May 15, 8 Marks**

Q. 4.6.7 Explain Secure Socket Layer handshake protocol in brief. (Ref. Sec. 4.6.2(A)) **May 16, Dec. 16, 5 Marks**

- As the name suggests when we meet to our friend/colleagues, we have habit to say hi/hello and do the *shake-hands* with each other before starting our actual communication. SSL handshake protocol uses somewhat same ideology but in terms of client and server.
- The first sub-protocol of SSL called *handshake protocol* used for secure communication between client and the server using an SSL enabled connections.
- In this protocol client authentication to the server is more important that server authentication because server has different options available for client authentication.
- The details **steps of SSL handshake protocol** are shown in Fig. 4.6.4.

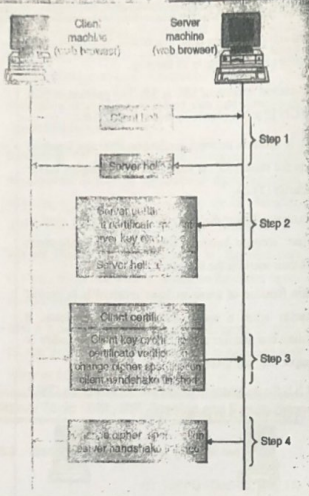

Fig. 4.6.4 : SSL handshake protocol

1. It is used by client and server to start communication over SSL enabled connection.
2. The handshaking is done 4 phases.

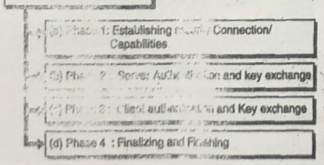

Fig. 4.6.5 : Phases of handshaking

(a) Phase 1 : Establish Security Connection/ Capabilities

This is used to establish security capabilities between client and server and capabilities associated with that connection. It consists of two messages, the client hello and the server hello.

Client hello

The client hello message contains the following parameters.

(i) The highest SSL version number which the client can support.

(ii) A 32-bit timestamp and a 28-byte random field that together serve as nonce during key exchange to prevent re- play attacks

(iii) A session id that defines the session (a variable length session identifier).

(iv) There is a cipher suite parameter that contains the entire list of cryptographic algorithms which supports client's system.

(v) A list of compression methods that can be supported by client.

Server

(i) The SSL version number, the highest among both SSL number of client and server, will be supported by client and other will be supported by server.

(ii) A 32 byte random number that will be used for master secret generation, however this random number is totally independent from the random number of client.

(iii) A session id that defines the session.

(iv) A cipher suite contains the list of all cryptographic algorithms that is sent by the client from which the server will select the algorithm

(v) A list of compression methods sent by the client from which the server will select the method.

➔ **(b) Phase 2 : Server Authentication and Key Exchange**

- In this phase, the server authenticates itself if it is needed. The server sends its certificate, its public key, and also request certificate (digital certificate) from the client.
- **Certificate :** The server sends a certificate message to authenticate itself to the client. If the key exchange algorithm is Diffie-Hellman then no need of authentication.
- **Server key Exchange :** This is optional. It is used only if the server doesn't sends its digital certificate to client.
- **Certificate Request :** The server can request for the digital certificate of client. The client's authentication is optional.
- **Server Hello done :** The server message hello done is the last message in phase 2. This indicates to the client that the client can now verify all the certificates received by the server. After this hello message done, the server waits for the client's side response in phase 3.

➔ **(c) Phase 3 : Client Authentication and Key Exchange**

- In this phase, the client authenticates itself if it is needed. The client sends its certificate, client key exchange and certificate verify to the server.
- **Certificate :** Client certificate is optional, it is only required if the server had requested for the client's digital certificate. If client doesn't have client's digital certificate it can send no certificate message or an Alert message to the server. Then it is upto server's decision whether to continue with the session or to abort the session.
- **Client key Exchange :** The client sends a client key exchange, the contents in this message are based on key exchange algorithms between both the parties.
- **Certificate verify :** It is necessary only if the server had asked for client authentication. The client has already sent its certificate to the server. But additionally if server wants then the client has to prove that it is authorized holder of the private key. The server can verify the message with its public key which was already sent to ensure that the certificate belongs to client.

➔ **(d) Phase 4 : Finish**

The client and server send messages to finish the handshaking protocol. It contains 4 steps. The first two messages are from the client i.e. change cipher specs, finished. The server responds back with change cipher spec and finished.

- **Change cipher spec :** It is a client side message telling about the current status of cipher protocols and parameters which has been made active from pending state.
- **Finished :** This message announces the finish of the handshaking protocol from client side.
- **Change Cipher spec :** This message is sent by server to show that it has made all the pending state of cipher protocols and parameters to active state.
- **Finished :** This message announces the finish of the handshaking protocol from server and finally handshaking is totally completed.

Syllabus Topic : Alert Protocol

4.6.2(B) Alert Protocol

- SSL uses the Alert protocol for reporting error that is detected by client or server, the party which detects error sends an alert message to other party. If error is serious then both parties terminate the session.
- Table 4.6.1 shows the types of alert messages. SSL alert protocol is the last protocol of SSL used transmit alert : (warnings, errors, fatal etc.) if any via SSL record protocol to the client or server.
- The SSL alert protocol format is shown in Fig. 4.6.6. Alert protocol uses two bytes to generate alert. First 1 byte indicates two values either 1 or 2. "1" value indicate warning and "2" value indicate a fatal error (if fatal error terminate the session/ connection).
- Whereas second 1 byte indicates predefined error code either the server or client detects any error it sends an *alert* containing the error (error occurred during handshaking, error occurred during data processing at server or client side, certificate defeats, etc.)

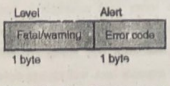

Fig. 4.6.6 : SSL Alert protocol

Table 4.6.1 : Types of alert messages

Alert Code	Alert Message	Description
0	close_notify	No more message from sender
10	unexpected_message	An incorrect message received
20	bad_record_mac	A wrong MAC received
30	decompression_failure	Unable to decompress.
40	handshake_failure	Unable to finalize handshake by the sender.
42	bad_certificate	Received a corrupted certificate.
42	Nocertificate	Client has no certificate to send to server.
42	Certificate expired	Certificate has expired.

Syllabus Topic : Record Protocol

4.6.2(C) Record Protocol

- After completion of successful SSL handshaking the keen role of SSL record protocol starts now.
- SSL record protocol is second sub-protocol of SSL also called lower level protocol.
- As defined earlier the SSL Record Protocol is responsible for encrypted data transmission and encapsulation of the data sent by the higher layer protocols (handshake, alert, HTTP) also to provide basic security services to higher layer protocols.
- SSL record protocol is basics for data transfer and specially used to build a data path between client and server and encrypt the data path before communication.
- SSL record protocol provides different service like data authentication, data confidentiality though encryption

algorithms and data integrity through message authentication (MAC) to SSL enabled connections.

- The details steps involved in SSL record protocol and SSL record header format as shown in Fig. 4.6.7.

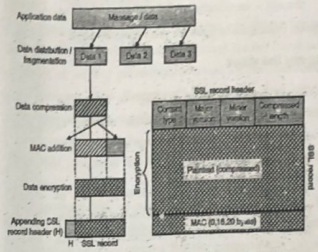

Fig. 4.6.7 : Record protocol and record header

- At this stage all necessary authentication and cryptographic parameters are exchanged between client and server now it's time of secure SSL data transmission through SSL record protocol.
- SSL record protocol takes application data i.e. actual data that client wants to send over server. Divide this data into the different blocks for each length should not exceed 16384 bytes this process is called as *data distribution* or *data fragmentation*.
- Next step is Data compression using lossless compression techniques; compression size of data should not exceed 1024 bytes.
- After the data fragmentation and compression step the MAC ((Message Authentication Code) is computed over the data and MAC is then appended to the compressed data (the data is now encapsulated) to form a new encrypted data / payload.
- The compressed data and MAC again goes through data encryption process. SSL record protocol uses symmetric key cryptographic techniques like DES, triple DES, AES, and IDEA because these techniques are specially designed to operate on block cipher.
- Finally SSL record header is prepended onto each encrypted blocks obtained from encryption process.
- Each output block produced by the SSL Record Protocol is referred to as an SSL record. The length of a record is not to exceed 32, 767 bytes.
- **SSL record header** (Refer Fig 4.6.7) consists of 8-bit content type to which identify nature of the message whether any application data or connection termination or any error message.
- Next field is Major Version which is 8-bit field used to indicate latest version of SSL is in use (e.g., 3). Minor Version which is 8-bit field indicates the lowest version of SSL is in use (e.g., 0).
- Plaintext (compressed) / compressed length which is 16-bit field indicates the length of the plaintext being compressed.
- Finally sends SSL layer encrypted data to TCP and IP (Transport and Internet layer) for necessary transmission over network
- At the receiver end, the encrypted blocks are decrypted and then checked for data authentication, data confidentiality and data integrity, reassemble these data into single unit, and delivered to the application-layer protocol.
- The Record Protocol provides **two services** in SSL connection :
  a) **Confidentiality :** This can be achieved by using secret key, which is already defined by handshake protocol.
  b) **Integrity :** The handshake protocol defines a shared secret key that is used to assure the message integrity.

Following are the **operations** performed in Record protocol after connection is established and authentication is done of both client and server.

1. **Fragmentation :** The original message that is to be sent is broken into blocks. The size of each block is less than or equal to 2^{14} (16384) bytes.
2. **Compression :** The fragmented blocks are compressed which is optional. It should be noted

that the compression process must not result into loss of original data.

3. **Addition of MAC :** The Message authentication code (a short piece of information used to authenticate a message for integrity and assurance of message) for each block is to be calculated using shared secret key.
4. **Encryption :** The overall steps including message is encrypted using symmetric key but the encryption should not increase the overall block size.
5. **Prepend Header :** After all the above operations, header is prepended in the encrypted block which contains following fields :

- Content type (8 bits) specifies which protocol is used for processing.
- Major Version (8 bits) specifies the major version of SSL used, for example if SSL version 3.1 is in use than this field contains 3.
- Minor Version (8 bits) specifies the minor version of SSL used, for example if SSL version 3.0 is in use than this field contains 0.
- Compressed length (16 bit) specifies the length in bytes of the original plain text block.

4.6.3 Transport Layer Security (TLS)

Q. 4.6.9 Explain TLS. (Ref. Sec. 4.6.3)

It is an extension of secure socket layer. The main aim of TLS is to provide security and data at the transport layer between two web applications. Almost all web browsers and web servers support TLS. It ensures no eavesdropping and tampering of the message.

- **The TLS protocol consists of two main components :** Handshake protocol, to start session and share private key, and Record protocol, to transmit data securely using the shared keys.
- **Handshake protocol :** In the Handshake protocol, both sending and receiving parties acknowledge their protocol versions, agree on cryptographic and compression algorithms, optionally authenticate each other through certificates, and use public-key encryption techniques to generate shared private keys.

Following are the steps

Step 1 : Clients sends message publicly to containing version of TLS,32-byte random number r_A consisting of a 4-byte timestamp and a 28-byte random number.

A Cipher Suite list in decreasing order of preference for each of the following algorithm families : Public-Key Algorithm (PKA), encryption algorithm used in the Cipher Block Chaining, and compression algorithm (COMPRESS).

Step 2 : Server informs the client about the decided algorithms (after examining the Cipher Suite list sent by the client) along with a 32-byte random number r_B constructed similarly as r_A.

Step 3 : Client replies with a number called pre-master secret s_{pm} using the public key algorithm PKA with public keys retrieved from the server's certificate signed by a Certifying Authority (CA).

Step 4 : Both parties independently calculate the 48-byte long master secret, s_m, to further obtain the keys to exchange data. The master secret is calculated using Pseudorandom Function

$PRF: s_m = PRF(s_{pm}, \text{"master secret"}, r_A||r_B)$

It is worth mentioning that in the previous version of TLS the master secret was computed as follows, before MD5 proven to be insecure :

$MD5(s_{pm}||SHA\text{-}1(A||s_{pm}||r_A||r_B)) \quad ||MD5(s_{pm}||SHA\text{-}1(BB||spm||rA||rB)) \quad ||MD5(s_{pm}||SHA\text{-}1(CCC||s_{pm}||r_A||r_B))$

Where A, BB, and CCC are strings added for padding.

Step 5 : At this stage, both parties know s_m, s_{pm}, r_A, and r_B, they independently compute the Key Block (KB) that contains all needed private shared keys for this session : $KB = P\ RF(s_m, \text{"key expansion"}, r_A||r_B)$ KB is then broken into six pieces and labeled as K1, K2, ..., and K6, before terminating the Handshake phase

- **Record protocol :** Now the client and the server are ready to communicate securely using the key block as a set of security parameters obtained by the Handshake protocol. The Record protocol takes data to be transmitted in one endpoint, fragments the data into manageable blocks, compresses the data, applies a MAC, encrypts by block cipher, and transmits the result. Received data is then decrypted, verified, decompressed, reassembled, and then delivered to higher-level application on the other endpoint. In short, Record protocol ensures that the connection is private via symmetric encryption by session unique keys and reliable via integrity check. Suppose the client wants to send data chunk, d.

The client

1. Compresses the data using the agreed algorithm : $d' = COMPRESS(d)$.
2. Hashes the compressed data for data integrity using K_2: $d'' \{d', HMAC_{K2}(d')\}$.
3. Encrypts the data along with its MAC using CBC mode block cipher BCA where the secret key is K_1 and the initialization vector is K_3: $d''' = BCA_{K1}(d'' K_3)$.
4. Sends d''' over the public channel.

And the server retrieves d from d'''

1. Decrypts the data along with its MAC using BCA_{K1}.
2. Verifies data integrity by computing HMAC of data using K_2 and comparing it with the HMAC computed on the client side.
3. Decompresses to retrieve d.

The process is reversed when server wants to send data to the client while the last three pieces of the key block is used instead.

Syllabus Topic : Electronic Mail Security - Pretty Good Privacy

4.7 Electronic Mail Security : Pretty Good Privacy

→ (SPPU - Dec. 13, Dec. 14, May 15)

Q. 4.7.1 Write short note on PGP. (Ref. Sec. 4.7) Dec. 13. 6 Marks

Q. 4.7.2 Write short note on Email security. (Ref. Sec. 4.7) Dec. 14. 4 Marks

Q. 4.7.3 What is PGP? Explain operations of PGP. (Ref. Sec. 4.7) May 15. 8 Marks

- We all are aware that most popular use of Internet is to send the email and chatting with the friend's, partner etc. But have you ever think that if we are sending mail to intended person is going in his inbox only?
- Security concerns have estimated that only about one in every 100 messages is secured against interception and modification attacks. Are we aware that sending an email to business partner or friends in clear text message is going through thousands of machines (between sender and receiver before it reaches to intended recipients?) these machines might read and saved the contents of email for future use?
- Many people think that name given in sender of the mail identifies who actually sends it.
- When you send a message through email, we cannot guarantee that it will be deliver to correct destination or received exactly what you sent. And even there is a no way of knowing that the message is received read and forwarded by attacker.
- Because of wide spared problem of email modifications, sending it to wrong destination by intermediate parties, email spoofing, we need a competing solution to overcome and address the issues of authentication, integrity and reliability of the messages between sender and receiver.

- The public key cryptography play an important role because of two keys used, only intended sender can decrypt the message using his public key as message encrypted using private key of the sender.
- The solution is called as Pretty Good Privacy (PGP) program/ software which provide the secrecy and non-repudiation of data sent over Internet especially by email.
- Pretty Good Privacy (PGP) is a popular open-source freely available software package/ techniques used to encrypt and decrypt email messages over the Internet.
- PGP is an e-mail security program written by Phil Zimmermann in 1991, PGP program become a de facto standard for e-mail security used to store the encrypted files so that it can be non-readable by other users or intruders.
- This program also be used to send an encrypted digital signature, let the receiver verify the sender's identity and know that the message was not changed or modified while transmission.
- Once the file is encrypted using PGP program only the intended recipient can decrypt it. Once message content digitally singed by sender, the sender guarantee to the recipients that message or file comes from valid sender and not by attacker.
- Digital signature functionality of PGP guarantees that the message or file come from the sender and not from an intruder.

4.7.1 Working of Pretty Good Privacy

→ **(SPPU - Dec. 14, Dec. 16, May 17)**

Q. 4.7.4 What are the different principal services provided by PGP? Discuss each service in detail. (Ref. Sec. 4.7.1) **Dec. 14. 8 Marks**

Q. 4.7.5 Explain working of PGP in detail. (Ref. Sec. 4.7.1) **Dec. 16. 9 Marks**

Q. 4.7.6 Explain working of PGP algorithm in detail. (Ref. Sec. 4.7.1) **May 17. 9 Marks**

- As mentioned earlier PGP uses the concept of public key cryptography, if user encrypts the plain text message using PGP, it first compress the plain text message.
- BGP uses data compression technique to encrypt the plain text message which saves the transmission time and disk space and more important it strengthen the security.
- After data compression PGP generate the session key. Table 4.7.1 shows how PGP encrypt the message in order to achieve the confidentiality, integrity and non-repudiation.

Table 4.7.1 : Encryption and Decryption of Pretty Good Privacy

Sr. No.	Parameter	Algorithm	Description
1.	Digital signature	SHA or RSA	A hash code of a message is created using SHA-1. This message digest is encrypted using RSA with the sender's private key and added with the message.
2.	Message encryption	IDEA or Triple DES with Diffie-Hellman or RSA	A message is encrypted using IDEA or 3DES with a one-time session key generated by the sender. The session key is encrypted using Diffie-Hellman or RSA with the recipient's public key and Rdded with the message.
3.	Compression	ZIP	A message is compressed, which saves the transmission time and disk space.

Sr. No.	Parameter	Algorithm	Description
4.	Email compatibility	Radix 64 conversion	For email applications transparency, an encrypted message converted to an ASCII string using Radix 64 conversion.
5.	Segmentation		To resemble the segments before decryption process.

Following are the detail encryption and decryption steps of PGP :

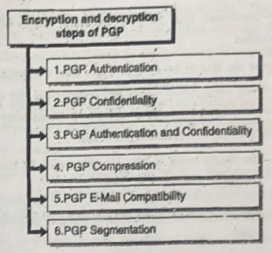

Fig. 4.7.1 : Encryption and decryption steps of PGP

→ **1. PGP Authentication**

1. Ramesh has (private/public) key pair *(Rd/Re)* and he wants to send a digitally signed message *m* to Suresh.
2. Ramesh hashes the message using SHA-1 to obtain *SHA(m)*.
3. Ramesh encrypts the hash using his private key *Rd* to obtain ciphertext *c* given by

   $c = \text{encrypt}_{Rd}(\text{SHA(m)})$
4. Ramesh sends the pair *(m,c)to Suresh*
5. Suresh receives *(m,c)* and decrypts *c* using Ramesh's public key *Re* to obtain signature *S*

   $S = \text{decrypt}_{Re}(c)$
6. He computes the hash of *m* using SHA-1 and if this hash value is equal to S then the message is authenticated.

Suresh is sure that the message is correct and that came from Ramesh. Furthermore Ramesh cannot later deny sending the message since only Ramesh has access to his private key *Rd* which works with respective public key *Rd*.

→ **2. PGP Confidentiality**

1. Ramesh wishes to send Suresh a confidential message *m*.
2. Ramesh generates a random session key *k* for a symmetric cryptosystem.
3. Ramesh encrypts *k* using Suresh's public key *Be* to get

   $k' = \text{encrypt}_{Be}(k)$
4. Ramesh encrypts the message *m* with the session key *k* to get ciphertext*c*

   $c = \text{encrypt}_{k}(m)$
5. Ramesh sends Suresh the values *(k',c)*
6. Suresh receives the values *(k',c)* and decrypts *k'* using his private key B_d to obtain *k*.

   $k = \text{decrypt}_{Bd}(k')$
7. Suresh uses the session key *k* to decrypt the ciphertext *c* and recover the message *m*

   $m = \text{decrypt}_{k}(c)$

Public and symmetric key cryptosystems are combined in this way to provide security for key exchange and then efficiency for encryption. The session key *k* is used only to encrypt message *m* and is not stored for any length of time.

→ **3. PGP Authentication and Confidentiality**

The schemes for authentication and confidentiality can be combined so that Ramesh can sign a confidential message which is encrypted before transmission. The steps required are as follows :

1. Ramesh generates a signature *c* for his message *m* as in the Authentication scheme

   $c = \text{encrypt}_{Rd}(\text{SHA(m)})$

2. Ramesh generates a random session key k and encrypts the message m and the signature c using a symmetric cryptosystem to obtain ciphertext C

$$C = encrypt_k(m,c)$$

3. He encrypts the session key k using Suresh public key

$$k' = encrypt_{Pu}(k)$$

4. Ramesh sends Suresh the values (k', C)
5. Suresh receives k' and C and decrypts k' using his private key Bd to obtain the session key k

$$k = decrypt_{Bd}(k')$$

6. Suresh decrypts the ciphertext C using the session key k to obtain m and c

$$(m, c) = decrypt_k(C)$$

7. Suresh now has the message m. In order to authenticate it he uses Ramesh public key Re to decrypt the signature c and hashes the message m using SHA-1.

If $SHA(m) = decrypt_{Re}(c)$

Then the message is authenticated.

➜ 4. PGP Compression

PGP can also compress the message if desired. The compression algorithm is ZIP and the decompression algorithm is UNZIP.

1. The original message m is signed as before to obtain

$$c = encrypt_{Bd}(SHA(m))$$

2. Now the original message m is compressed to obtain

$$M = ZIP(m)$$

3. Ramesh generates a session key k and encrypts the compressed message and the signature using the session key

$$C = encrypt_k(M,c)$$

4. The session key is encrypted using Suresh's public key as before.
5. Ramesh sends Suresh the encrypted session key and ciphertext C.
6. Suresh decrypts the session key using his private key and then uses the session key to decrypt the ciphertext C to obtain M and c

$$(M,c) = decrypt_k(C)$$

7. Suresh decompresses the message M to obtain the original message m

$$m = UNZIP(M)$$

8. Now Suresh has the original message m and signature c. He verifies the signature using SHA-1 and Ramesh's public key as before.

➜ 5. PGP E-Mail Compatibility

- Many electronic mail systems can only transmit blocks of ASCII text. This creates a problem when sending encrypted data which is in cipher text form might not correspond to ASCII characters that can be transmitted.
- PGP overcomes this problem by using **Radix-64 conversion**.
- Suppose the text to be encrypted has been converted into binary using ASCII coding and encrypted to give a cipher text stream of binary. Radix-64 conversion maps arbitrary binary into printable characters.
  1. The binary input is split into blocks of 24 bits (3 bytes).
  2. Each 24 block is then split into four sets each of 6-bits.
  3. Each 6-bit set will then have a value between 0 and $2^6 - 1$ (= 63).
  4. This value is encoded into a printable character.

➜ 6. PGP Segmentation

- Another constraint of e-mail is that there is usually a maximum message length.
- PGP automatically blocks an encrypted message into segments of an appropriate length. On receipt, the segments must be re-assembled before the decryption process.
- Following are the service offered by the PGP:

1.	Authentication	2.	Confidentiality
3.	Non-repudiation	4.	Integrity
5.	Compression	6.	E-mail compatibility
7.	Segmentation		

4.7.2 Backdoors and Key Escrow in PGP

➜ (SPPU - May 16)

Q. 4.7.7 What is Backdoors and Key Escrow in PGP ? (Ref. Sec. 4.7.2) **May 16, 9 Marks**

- Suppose, we have saved your password in laptop. So, anyone who has access the laptop, can get unauthorized access to your account. And that is a simple way of saying what a **Backdoor** is.
- A **Backdoor** is a method for bypassing normal authentication in a system and thus, provide unauthorized remote access to the system to malicious users.
- A backdoor is a "feature" in the software of PGP like an utility functions but not in the encryption algorithm that allows an outside party to decrypt which is encrypted by PGP.
- A Backdoor may be implemented as a hidden part of a program or a separate program or even be implemented by hardware.
- Just to give an example, in 2003 a Backdoor was planted in Linux Kernel. In a conditional statement for checking root access permission, '==' was replaced with '='. As a result, it gave unauthorizd access to malicious callers. Even very recently, in 2015, **Juniper Netwerks** have warned about a malicious Backdoor in their firewalls that automatically decrypts VPN traffic.
- There are two types of Backdoors – **Object Code Backdoors** and **Asymmetric Backdoors**.
- In **Object Code Backdoors**, software source code remains unchanged, but the object code gets modified maliciously. As the object code is designed to be machine readable, it becomes much more difficult to detect. These type of Backdoors are inserted in the on-disk object code or inserted at some point during compilation, linking or loading.
- Recompiling the software source code may get rid of the Backdoors. So, malicious users sometimes change the compiler source code in such a way that, whenever it compiles, links and loads the source code, the Backdoor is inserted. These Backdoors can be fixed by recompiling the compiler and removing the Backdoor inserting codes.
- Normally, Backdoors are symmetric. Anyone who finds the Backdoor, can in turn use it. But, **Asymmetric Backdoors** can be exploited only by the attacker who plants it, even if the Backdoor implementation becomes public. This type of attacks are termed as **Kleptography** and they can be carried out in software, hardware or in combination of both. The theory of Asymmetric Backdoors is a part of a larger field named **Cryptovirology**.

☞ Counter measures

- Once Backdoors are detected, rebuild a clean system and transfer data.
- Another method is to use Diverse Double Compiling or DDC. It requires a different compiler and the source code of the compiler to be tested. That source code, while compiled with two different compilers, would result in two different stage-1 compilers showing same behaviour.
- Thus, the same source code compiled in two different stage-1 compilers, must result in two identical stage-2 compilers. This method was applied to verify that C compiler of GCC Suite contained no Trojan, using the ice as the other compiler. Normally, Operating Systems vendors implement these type of methods to make sure they are not distributing a compromised system.

☞ Key Escrow

- Key escrow is a cryptographic key exchange process in which a key is held in escrow, or stored, by a third party. A key that is lost or compromised by its original user(s) may be used to decrypt encrypted material, allowing restoration of the original material to its unencrypted state.
- Key escrow systems provide a backup source for cryptographic keys. Escrow systems are somewhat risky because a third party is involved.

- The Clipper Chip was a U.S. government encryption chipset introduced in 1993. The chipset was promoted as an encryption device with a government-held (escrow) master key to facilitate encryption in the face of security threats. The controversial Clipper Chip was defunct by 1996, but the concept evolved into the Pretty Good Privacy (PGP) encryption tool, which is used worldwide.
- **Key escrow** (also known as a "fair" cryptosystem) is an arrangement in which the **keys** needed to decrypt encrypted data are held in **escrow** so that, under certain circumstances, an authorized third party may gain access to those **keys**.

Syllabus Topic : S/MIME

4.8 S/MIME

→ **(SPPU - Dec. 13, May 15)**

Q. 4.8.1 Describe the functions of S/MIME. Also describe the functions of Cryptographic Algorithms used in S/MIME. (Ref. Sec. 4.8) **Dec. 13, 10 Marks**

Q. 4.8.2 Write a short note on S/MIME. (Ref. Sec. 4.8) **May 15, 4 Marks**

- S/MIME stands for Secure/Multipurpose Internet Mail Extensions provides a de facto standard to send and receive secure Multipurpose Internet Mail Extensions (MIME) data.
- S/MIME developed by RSA Data Security, S/MIME version 3 is now being maintained by the S/MIME Working Group of the Internet Engineering Task Force (IETF).
- As explained in PGP, because of large number of increasing Internet usage for sending and receiving emails over an insecure communication channel increases the risk of data modification, confidentiality, authentication and non-repudiation.
- We need our mail should be safe from unauthorized users. It should reach to intended recipients only. Based on the popular Internet usage, S/MIME provides the different cryptographic security services to secure electronic messaging applications: authentication, message integrity and non-repudiation and data security.
- Traditional mail user agents (MUAs) uses S/MIME to add cryptographic security services to mail that is sent, and to interpret cryptographic security services in mail that are received.
- S/MIME uses both symmetric as well as asymmetric key cryptographic techniques to sign and encrypt e-mail. Sender as well as receiver of the mail has two keys: A private key, which is kept secret and a public key, which is available to everyone. Mails encrypted using senders private key can only be decrypted using his public key and vice versa.

Mail signing concepts

- Generally when sender sends a message he could just encrypt the message using his private key at the receiver side. If the message decrypted using senders public key then we can say that the message came from authenticated user and its content cannot be modified, because a message, that can be decrypted using senders public key must have been encrypted using senders private key only. To increase the performance S/MIME uses the following concepts.
- The message is not encrypted using receivers public key instead of that it is encrypted using a randomly created symmetric session key because symmetric key is faster than asymmetric key cryptography.
- The generated session key is encrypted using receiver's public key so that only receivers can retrieve the session key and thus decrypt the original message.
- The following steps are taken in order to create an encrypted message :
  1. The user writes the message in plain text.
  2. Triple DES algorithm is used to create random session key.
  3. The message is being encrypted using the random session key.
  4. For every recipient, the session key is being encrypted using the recipient's public key.

- S/MIME-e-mail software must support Secure Hash Algorithms (SHA-1) standard and Message Digest Algorithm (MD5) in order to provide backward-compatibility with MD5-digested S/MIME v2 messages.

Table 4.8.1 : Contents of encrypted mail

Encrypted Mail	
Message encryption	Message encrypted with the session key.
Session key encryption	Session encrypted with the recipient's public key can only be decrypted using his private key only.
Identify algorithm	To tell receiver which decryption algorithm used..
Sender's public key	To enable the recipient to encrypt his response.

- **Digital signatures :** To encrypt the message digest, the S/MIME client must support DSS (Digital Signature Standard) and should support RSA (Rivest, Shamir, Adleman)
- **Content Encryption:** To encrypt the message content (symmetrically, using a random session key), Triple DES must be supported
- **Key encryption and management :** To encrypt the session key, Diffie-Hellmann algorithm must be supported. Key S/MIME uses X.509v3 certificates to determine whether a public key used to verify a signature is trustworthy. The certificate signed by Certificate Authority (CA) for claiming that public key belongs to the person.
- S/MIME (Secure/Multipurpose Internet Mail Extensions) is a specification for secure electronic mail providing authentication and confidentiality. It is not a particular software product but a standard designed to be implemented by various e-mail vendors, so that any two S/MIME-supporting mail clients can communicate securely.

Syllabus Topic : Secure Electronic Transaction

4.9 Secure Electronic Transaction (SET)

→ **(SPPU - Dec. 13, May 15, May 16)**

Q. 4.9.1 Explain key features of SET. (Ref. Sec. 4.9)

Q. 4.9.2 With help of diagram explain SET Participants. (Ref. Sec. 4.9) **Dec. 13, 8 Marks**

Q. 4.9.3 Explain working principles of SET with suitable diagram. (Ref. Sec. 4.9) **May 15, 8 Marks**

Q. 4.9.4 What is secure Electronic Transaction ? (Ref. Sec. 4.9) **May 16, 6 Marks**

- SET stands for Secure Electronic Transaction. It is an encryption and security specification protocol designed to protect credit card transactions over an insecure channel such as Internet.
- SET is not a payment system it is set of rules and regulations designed to protect credit card payments of users, employee over an open network such as Internet in a secure way.
- SET was developed in 1996 by VISA and MasterCard, with participation from different leading technology companies, which includes Microsoft, IBM, Netscape, RSA, Teresa Systems and VeriSign.

After testing of the SET in 1998 it declares as a standard for safeguarding credit card purchases made over open networks and made it available to users with following requirements.

- SET create a secure communications channel among all parties involved in a transaction.
- SET provides privacy because the information is only available to sender, receiver and bank or the communication parties' involved in transaction.
- SET provides confidentially, only sender and his intended receiver should be able to access the contents of a message. It assures to card holder is that is safe and accessible only to the intended recipient.
- SET provides integrity of the message. Integrity gives assurance that data received exactly as sent by an authorized entity. (No alteration, no modification, no deletion and no intersection etc.).

4.9.1 SET Participants

→ (SPPU - May 17)

Q. 4.9.5 List and explain various participants involved in Secure Electronic Transaction (SET). (Ref. sec. 4.9.1) May 17. 5 Marks

Following are the components of the Secure Electronic Transaction (SET) which involves in the electronic payment as shown in Fig. 4.9.1.

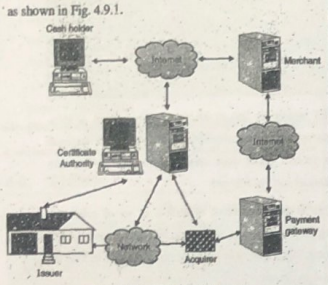

Fig. 4.9.1 : SET Participants

- **The cardholder :** called as buyer in the transaction who initiates the transaction.
- **The merchant :** Also called seller of goods and services which maintains an account with a bank or acquirer.
- **The acquirer :** Also known as bank or financial institution. The financial institution that establishes an account with a merchant and processes payment card authorizations and payments.
- **The issuing bank :** Bank that maintains the account of the buyer and issues a credit card to the buyer and also sets limit on the amount of purchases.
- **Certification Authority (CA) :** Certification Authority (CA) is a trusted unit that helps to issue certificates.
- A CA takes the certificate request from owner, verifies the requested information according to the terms and conditions of the CA, and uses its private key to apply digital signature to the certificate.
- Responsibility of the CA is to identify the correct identity of the person who asks for a certificate to be issued, and make sure that the information contained within the certificate is legal and later digitally sign on certificate.
- This is an entity that is trusted to issue X.509v3 public-key certificates for cardholders, merchants, and payment gateways.
- **Payment gateways :** It is designated third party that processes merchant payment messages. The merchant exchanges Secure Electronic Transaction messages with the payment gateway over the Internet, while the payment gateway has some direct or network connection to the acquirer's financial processing system.
- Following are the steps of interactions used in SET protocol :

1. **The customer opens the account :** Once the customer obtains a credit card account, such as MasterCard or Visa, from the bank which supports electronic payment and Secure Electronic Transaction then customer may proceed for future communication over network.
2. **The customer receives a certificate :** After suitable verification of identity, the customer receives an X.509v3 digital certificate, which is signed by the bank which verifies the customers RSA public key and its expiration date.
3. **Merchants have their own certificates :** A merchant have two public keys one for signing message and another for key exchange. The merchant also needs a copy of the payment gateway's public-key certificate.
4. **The customer places an order :** Here customer first browsing through the merchant's Web site to select items and determine the price. The customer now sends its list of items to be purchased to the merchant. Upon receiving list of items from customer merchant returns an order from containing the list of items, their price, a total price, and an order number to the customer.

5. **The merchant is verified :** Along with order number, the merchant sends a copy of its certificate, so that the customer can verify that he or she is dealing with a valid merchant store.
6. **The order and payment is verified :** The customer sends both order and payment information to the merchant, along with the customer's certificate (approved by CA). Customer also confirms the purchase of the items in the order form. The payment contains credit card details. The payment information is encrypted in such a way that it cannot be read by the merchant. The customer's certificate enables the merchant to verify the customer.
7. **The merchant requests payment authorization:** The merchant sends the payment information to the payment gateway for authentication as well as to check whether customer's available credit is sufficient for this purchase.
8. **The merchant confirm the order :** Upon receiving payment confirmation from customers credit, the merchant sends confirmation of the order to the customer.
9. **The merchant provides the goods or service :** After all verification the merchant provides the goods or service to the customer.
10. **The merchant request payment :** This request is sent to the payment gateway, which handles all of the payment processing.

☞ **MIME**

- S/MIME (for Secure MIME, or Secure Multipurpose Mail Extension) is a security process used for e-mail exchanges that makes it possible to guarantee the confidentiality and non-repudiation of electronic messages
- S/MIME is based on the MIME standard, the goal of which is to let users attach files other than ASCII text files to electronic messages.
- The MIME standard therefore makes it possible to attach all types of files to e-mails. S/MIME was originally developed by the company RSA Data Security.
- Ratified in July 1999 by the IETF, S/MIME has become a standard, whose specifications are contained in RFCs 2630 to 2633.
- The S/MIME standard is based on the principle of public-key encryption. S/MIME therefore makes it possible to encrypt the content of messages but does not encrypt the communication.
- The various sections of an electronic message, encoded according to the MIME standard, are each encrypted using a session key.
- The session key is inserted in each section's header, and is encrypted using the recipient's public key. Only the recipient can open the message's body, using his private key which guarantees the confidentiality and integrity of the received message.
- In addition, the message's signature is encrypted with the sender's private key. Anyone intercepting the communication can read the content of the message's signature, but this ensures the recipient of the sender's identity, since only the sender is capable of encrypting a message (with his private key) that can be decrypted with his public key.

Chapter Ends...

□□□

Unit V

CHAPTER 5

Intrusion and Firewall

Syllabus

Introduction, Computer Intrusions. Firewall Introduction, Characteristics and types, Benefits and limitations. Firewall architecture, Trusted Systems, Access Control. Intrusion detection, IDS : Need, Methods, Types of IDS, Password Management, Limitations and Challenges.

Syllabus Topic : Introduction, Firewall Introduction, Characteristics and Types, Benefits and Limitations, Firewall Architecture

5.1 Firewall Introduction

Q. 5.1.1 Write a short note on firewall. (Ref. Sec. 5.1)

Q. 5.1.2 What is firewall? (Ref. Sec. 5.1)

- Firewall is called as barrier place between inside and outside network to protect organization from inside and outside hackers. It also filters all traffic between intranet and extranet which runs through it.
- The main purpose of the firewall is to keep attackers outside the protected environment. For that policies are set in the firewall to decide what is allowed and what is not allowed.
- Moreover we can decide the allowed places, allowed users, allowed sites, can provide different access rights to different category of the users.
- **Example :** Cyber am through which only educational sites are allowed through college internet and non-educational sites like facebook, twitter can be blocked using firewall.

5.1.1 Firewall Characteristics

➔ **(SPPU - May 16, Dec. 16, May 17)**

Q. 5.1.3 What are the various characteristics of firewall ? (Ref. Sec. 5.1.1) May 16, Dec. 16, May 17, 5 Marks

- Following lists the characteristics as well as design goals for a firewall :
  1. All inside and outside traffic must pass through the firewall. This is possible only because of physically blocking of all access to the local network except via the firewall.
  2. The traffic defined by the local security policy will only allowed to pass through the network. Different types of firewall are used to define the policies as per the norms decided.
  3. The firewall itself is immune to penetration. Different techniques are used to control access and enforce the site's security policy.
- **Service control :** This policy helps to determine which type of internet services that can be accessed inbound and outbound. Firewall can filter traffic on the basis of IP address and TCP port number. It also act as proxy server that receives and interprets each service request before passing it on.

- **Direction control :** Direction control determines the direction in which particular service requests may be initiated and allowed to flow through the firewall.
- **User control :** This technique is used to controls access to a service according to which user is attempting to access it.
- **Behaviour control :** Controls how particular services are used. For example, the firewall may filter e-mail to eliminate spam.

5.1.2 Limitations of Firewalls

Q. 5.1.4 What are the disadvantages of firewalls? (Ref. Sec. 5.1.2)

A firewall may be apivotal component of securing your organize and is planned to address the issues of information integrity or activity verification (through stateful packet inspection) and secrecy of your inner network (through NAT). Your network picks up these benefits from a firewall by accepting all transmitted activity through the firewall. Your network picks up these benefits from a firewall by receiving all transmitted activity through the firewall.

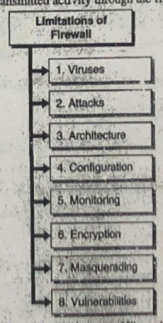

Fig. 5.1.1 : Limitations of Firewall

Following are the limitations of firewall :

➔ **1. Viruses**

Not all firewalls have full protection against computer viruses because virus uses different encoding techniques to encode files and transfer them over Internet.

➔ **2. Attacks**

A firewall cannot prevent users or attackers with modems from entering in to or out of the internal network, thus bypassing the firewall and its protection completely.

➔ **3. Architecture**

Firewall architecture depends upon single security mechanism failure. If that security mechanism has a single point of failure, affects on entire firewall programs which opens the loop falls for intruders.

➔ **4. Configuration**

Firewall doesn't have mechanism to tell administrator about incorrect configuration. Only trained professionals in the field of network security can configure firewall properly.

➔ **5. Monitoring**

Firewall doesn't give notification about hacking. It will notify only about threat occurrences. The reason is, organization demands additional hardware, software and different networking tools as per there requirement hence there is no control on it.

➔ **6. Encryption**

Firewall and Virtual Private Networks (VPNs) don't encrypt confidential documents and E-mail messages sent within the organization or to outsiders. Dignified procedures and tools are needed to provide protection against confidential documents.

➔ **7. Masquerading**

Firewalls can't stop hacker those who steal login id and password of authentic user to gain access to a secure network. Once attacker gains full access of the entire network, attacker can delete or change the network policies of organization.

8. Vulnerabilities

Firewall can't tell other venerability that might allow a hacker access to your internal network.

5.1.3 Firewall Architecture and Types

→ (SPPU - Dec. 14, May 15, May 16, Dec. 16, May 17)

Q. 5.1.5 What is packet filtering? Explain packet filtering gateway with suitable example. (Ref. Sec. 5.1.3) Dec. 14. 6 Marks

Q. 5.1.6 Explain with suitable example packet filter. (Ref. Sec. 5.1.3) May 15. 8 Marks

Q. 5.1.7 Explain Architecture of firewall. (Ref. Sec. 5.1.3) May 16. 6 Marks

Q. 5.1.8 Describe types of firewall. (Ref. Sec. 5.1.3) Dec. 16, May 17. 6 Marks

A firewall is a kind of reference monitor. All network traffic passes through firewall. That's why it is always in invoked condition. A firewall is kept isolated and cannot be modified by anybody other than administrator. Generally it is implemented on a separate computer through which intranet and extranets are connected.

Following are the common architectural implementations of firewalls :

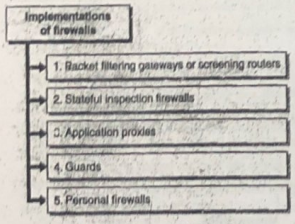

Fig. 5.1.2 : Implementations of firewalls

1. Packet Filtering Gateway

- It is the most simple and easy to implement firewall. Packet filtering is done on the basis of packets source or destination address or based on some protocol type like HTTP or HTTPs.
- If the firewall is placed just behind the router then the traffic can be analyzed easily. In the Fig. 5.1.3 it is shown that how packet filtering gateway can block traffic from network 1 and allow traffic from network 2.
- Also the traffic using telnet protocol is blocked. Packet filters do not analyze the contents of the packet rather they just check IP address of the packets as shown in Fig. 5.1.3.
- The biggest disadvantage of the packet filtering gateway is that it requires lot of detailing to set policies.

Example

- If port 80 is blocked. If some applications essentially need use of port 80 then in this case we have to provide all the details of those applications for which port 80 is needed.

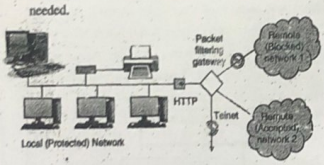

Fig. 5.1.3 : Packet Filter Blocking Addresses and Protocols

2. Stateful Inspection Firewall

- Packet filtering is done one packet at time. Sometimes attacker may use this technique for their attack. Attacker can split the script of attack into different packets so that the complete script of attack cannot be identified by packet filtering firewall.
- To avoid this stateful inspection firewall keeps record of states of the packets from one packet to another. Thus sequence of packets and conditions within the packets can be identified easily.

3. Application Proxies

- Packet filters cannot see inside the packets. From the packet headers they just get IP addresses for filtering.

- Application proxy is also known as a bastion host. Fig. 5.1.4 shows firewall proxies.

Example

- A college wants to publish a list of selected students. Then they just want students to read that list. No student can change that list. Moreover students cannot access more data than the list.
- Application proxy helps us in this regard. Here it helps us to check only list is displayed on the screen and not more than that. That list should not have any modified contents.

Proxies on the firewall can be customized as per the requirements.

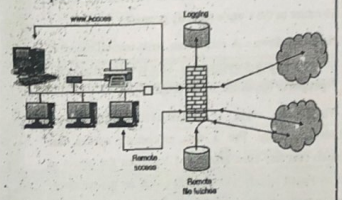

Fig. 5.1.4 : Firewall Proxies

4. Guard

- A guard is kind of complex firewall. It works similar to proxy firewall. Only difference is that guard can decide what to do on behalf of the user by using available knowledge.
- It can use knowledge of outside users identity, can refer previous interactions, blocked list etc.

Example

- In order to increase the speed of the internet a school can set download limit for the students.
- A student can download only 20mb data per day etc.

5. Personal Firewalls

Q. 5.1.9 What is personal firewalls? (Ref. Sec. 5.1.3(5))

- For a personal use to keep separate firewall on a separate machine is quite difficult and costly. So personal users need a firewall capability on lower cost.
- An application program which can have capabilities of a firewall can solve this problem.
- It can screen incoming and outgoing traffic on a single host.
- Symantec, McAfee, Zone alarm are the examples of personal firewalls. Personal firewalls can be combined with antivirus systems.

5.1.4 Firewall Configurations

→ (SPPU - Dec. 13)

Q. 5.1.10 How firewalls are configured and managed? (Ref. Sec. 5.1.4) Dec. 13. 4 Marks

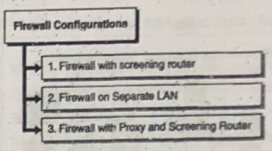

Fig. 5.1.5 : Firewall Configurations

1. Firewall with screening router

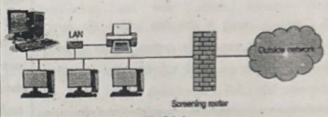

Fig. 5.1.6

The screening router is placed in between intranet and extranet. Another name for screening router firewall is network level or packet-filter firewall. Protocol attributes are used for performing the screening of incoming packets. The attributes like source or destination address, type of protocol, source or destination port, or some other protocol-specific attributes plays a vital role. A screening router performs packet-filtering and is utilized as a firewall. In a few cases a screening router may be utilized as perimeter assurance for the internal network or as the whole firewall solution.

2. Firewall on Separate LAN

Unauthorized internet users from accessing private networks connected to the internet are prevented by firewall, especially intranets. All messages entering or leaving the Intranet (i.e., the local network to which you are connected) must pass through the firewall, which examines each message and blocks those that do not meet the specified security constraint.

To overcome the problem of the exposure of LAN, a proxy firewall can be installed on its own LAN.

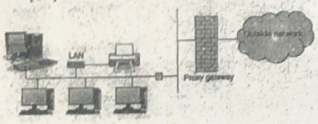

Fig. 5.1.7

3. Firewall with Proxy and Screening Router

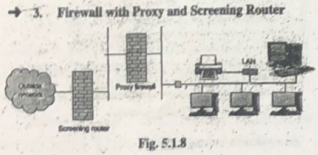

Fig. 5.1.8

If screening router is installed behind the proxy firewall, then it ensures the correct address to proxy firewall. In other words it is a double guard protection. If anyone fails LAN is not exposed.

Syllabus Topic : Trusted Systems

5.2 Trusted Systems

→ **(SPPU - May 16, May 17)**

Q. 5.2.1 What is Trusted System ? (Ref. Sec. 5.2) May 16, May 17, 5 Marks

Trusted system is level base security system where protection is provided and handled according to the different levels. This is commonly found in military, where information is categorized as unclassified (U), confidential (C), secret (S), top secret (TS), or beyond.

This concept is equally applicable in other areas, where information can be organized into categories and users can be granted clearances to access certain categories of data. When multiple categories or levels of data are defined, the requirement is referred to as **multilevel security**.

The general statement of the requirement for multilevel security is that a subject at a high level may not convey information to a subject at a lower or non-comparable level unless that flow accurately reflects the will of an authorized user. For implementation purposes, this requirement is in two parts and is simply stated. A multilevel secure system must enforce the following :

- **No read-up :** A subject can only read an object of less or equal security level. This is referred to in the literature as the **simple security property**
- **No write-down :** A subject can write into an object of greater or equal security level. This is referred to as the ***-property** (pronounced star property)

These two rules, if properly enforced, provide multilevel security. For a data processing system, the approach that has been taken, and has been the object of much research and development, is based on the **reference monitor** concept. The reference monitor is a controlling element in the hardware and operating system of a computer that regulates the access of subjects to objects on the basis of security parameters of the subject and object. The reference monitor has access to a file, known as the security kernel database that lists the access privilege (security clearance) of each subject and the protection attributes (classification level) of each object. The reference monitor enforces the security rules (no read-up, no write-down) and has the following properties:

- **Complete mediation :** The security rules are enforced on every access, not just, for example, when a file is opened (requires high performance overhead).
- **Isolation :** The reference monitor and database are protected from unauthorized modification (requires impossibility for attacker to change database).
- **Verifiability :** The reference monitor's correctness must be provable. That is, it must be possible to

demonstrate mathematically that the reference monitor enforces the security rules and provided complete mediation and isolation. If provided, system is referred to as a trusted system. These are stiff requirements.

Important security events, such as detected security violations and authorized changes to the security database, are stored in the audit file.

These are the systems whose failure may break a specified security policy. The base of the trusted system is as follows :

- It combines software and hardware portions with respect to security.
- It can act as a mediator.
- It is tamperproof.
- It is validated.

Syllabus Topic : Access Control

5.3 Access Control

→ **(SPPU - Dec. 16)**

Q. 5.3.1 What is Access control security service? (Ref. Sec. 5.3) Dec. 16, 5 Marks

Access Control is the ability to limit and control the access to the host systems. It prevents unauthorized use of a resource. The service used to prevent unauthorized use of a resources i.e. complete control over who can access to resources, under what conditions access can occur and what are different accessing methodology.

For example

It controls the access of resources which is to be made available only to legitimate user. Secondly it looks to the conditions of accessing the resource or network and what is allowed to be done to the resources.

Database administrator decides what should be stored in a database and to whom access rights can be given based on the needs of different users. Database administrator takes these decisions on the basis of access policies.

Following are the factors that the DBMS may consider for deciding access policies :

1. **Availability of Data :** While updating proper blocking and locking should be used so that other processes cannot interfere and can get correct data also.
2. **Acceptability of Access :** DBMS must protect sensitive data from unauthorized users.
3. **Assurance of Authenticity :** Sometimes database may permit some users to access sensitive data.

   Example : During auditing of a failure database may give permission to auditor/administrator also to access the sensitive data in order to resolve the problem after looking at the severity of the things.

Syllabus Topic : Intrusion Detection

5.4 Introduction to Intrusion Detection

- With the rapid expansion of Internet during recent years, security has becomes an essential issue for computer networks and computer systems.
- As defined earlier the main aim of a security system is to protect the most valuable assets (data/secret information) of an organizations like banks, companies, universities and many others, because these organizations have data or secret information in some form, and their security policies are keen for protecting the privacy, integrity, and availability of these valuable information or data.
- As these organizations will have different security policies and requirements depending on their vision and missions.
- Many efforts have been carried out to accomplish this task are security policies, firewalls, anti-virus software even *Intrusion Detection Systems* (IDSs) to configure different services in operating systems and computer networks.
- But still detecting different attacks (like denial service attacks, IP spoofing, ping of death, network scanning etc.) against computer networks is becoming a crucial

problem to solve in the field of cryptography and network security.

- To overcome all above problems researcher in the field of computer security came with existing but different solution called Intrusion Detection System (IDS). Before discussing on IDS let us understand some key points like what is intrusion? What is intrusion detection and then what is intrusion detection system?

5.4.1 Intrusion Detection

Q. 5.4.1 What are the strengths and limitations of Intrusion Detection System? (Ref. Sec. 5.4.1)

Q. 5.4.2 What is intruder and intrusion detection system? (Ref. Sec. 5.4.1)

- Before defining Intrusion Detection first understand what is an Intruder?
- An *Intruder* is a person who intercepts system availability, confidentiality and data integrity. Intruder's gains unauthorized access to a system with criminal intensions. Intruder may damage that system or disturbs data.
- When an attacker or intruder attempts to break into an information system or performs an illegal action such as denial of service attacks, scanning a networks, ping scan, sending many request for connection setup using fake IP address, etc. which is legally not allowed, that is called as an *intrusion*.
- *Intrusion detection* is an important technology that monitors network traffic, events and identifies network intrusions such as abnormal network behaviours, unauthorized network access and malicious attacks to computer systems.
- The general example of intrusion detection is when we suffer from some disease and asking doctor what happen to me. Doctor suggests for blood checking and sends blood sample to laboratory for detection.
- The blood report given by pathologies is just detection of disease (number of platelets count, WBC, RBC, haemoglobin, etc.) then after checking the entire history of blood report doctor suggests medicine to cure the disease.
- Here blood report is intrusion detection where as medicine given by the doctor after checking blood report is called intrusion detection system. Finally how fast patient get relief depends upon the doctor's education, experience and knowledge, joke apart let us move towards technical definition of IDS.

Syllabus Topic : Intrusion Detection System - Need, Methods

5.5 Intrusion Detection System : Need, Methods, Types of IDS

→ **(SPPU - Dec. 13, Dec. 14, May 15, May 16, May 17)**

Q. 5.5.1 What is Intrusion Detection System (IDS)? Explain different reasons for using IDS and different terminologies associated with IDS. (Ref. Sec. 5.5) **Dec. 13, 8 Marks**

Q. 5.5.2 What is IDS? Differentiate statistical Anomaly detection and rule base intrusion detection. (Ref. Sec. 5.5) **Dec. 14, 8 Marks**

Q. 5.5.3 What is intrusion detection system? Enlist and explain different types of IDS. (Ref. Sec. 5.5) **May 15, 8 Marks**

Q. 5.5.4 What are the challenges of intrusion detection? (Ref. Sec. 5.5) **May 16, May 17, 6 Marks**

- Intrusion Detection system has some policies or mechanisms to protect computer systems from many attacks. As the use of data transmission and receiving over the internet increases the need to protect the data of these connected systems also increases. Many scientists have different definition of IDS but as per our point of view IDS can be defined as below point.
- "An Intrusion Detection System is software that monitors the events occur in a computer systems or networks, analyzing what happens during an execution and tries to find out indications that the computer has been misused in order to achieve confidentiality, integrity and availability of a resource or data".
- The IDS will continuously run on our system in the background, and only generate the alert when it detects something suspicious as per its own rules and regulation or attack signature present into it and taking some immediate action to prevent damage.

Intrusion detection

- System examines or monitors system or network activity to find possible attacks on the system or network. Signs of violation of system security policies, standard security practices are analyzed.
- Intrusion Prevention is the process of detecting intruders and preventing them from intrusive effort to system.

Challenges of Intrusion Detection

In order to better understand intrusion detection systems, it is important to realize that threats to networked computer systems come in a number of forms. According to the source of threats, potential intruders can be roughly classified into two categories :

1. **Outside Intruders :** The attack is launched by an unauthorized computer user. The attacker will stole or broken passwords, using system vulnerabilities or improper configurations, human engineering techniques, to gain access to computers.
2. **Inside Intruders :** Internal intruders, who have permission to access the system with some restrictions, In this case, the intruder already has legitimate access to a computer system, but utilizes any of the previously mentioned techniques to gain additional privileges and misuse the computer system. Sometimes inside intruders are more harmful than outside intruders. It is observed that 80% of intrusions and attacks come from within organizations.

Following are the possible type of attacks that intrusion detection needs to face :

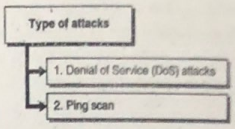

Fig. 5.5.1 : Type of attacks

→ **1. Denial of Service (DoS) attacks**

- These attacks attempt to *"shut down a network, computer, or process; or otherwise deny the use of resources or services to authorized users"*.
- There are two types of DoSattacks :
  - (i) Operating system attacks, which target bugs in specific operating systems and can be fixed with patches;
  - (ii) Networking attacks, which exploit inherent limitations of networking protocols and infrastructures.
- An example of operating system attack is teardrop,in which an attacker exploits a vulnerability of the TCP/IP fragmentation re-assembly code that do not properly handle overlapping IP fragments by sending a series of overlapping packets that are fragmented. Typical example of networking DoS attack is a "SYN flood" attack, which takes advantage of three-way handshake for establishing a connection. In this attack, attacker establishes a large number of "half-open" connections using IP spoofing. The attacker first sends SYN packets with the spoofed (faked) IP address to the victim in order to establish a connection.
- The victim creates a record in a data structure and responds with SYN/ACK message to the spoofed IP address, but it never receives the final acknowledgment message ACK for establishing the connection, since the spoofed IP addresses are unreachable or unable to respond to the SYN/ACK messages.

- Although the record from the data structure is freed after a time out p...od, the attacker attempts to generate sufficiently large number of "half-open" connections to overflow the data structure that may lead to a segmentation fault or locking up the computer.

2. Ping scan

- The simplest form of scan, an attacker sends an ICMP echo request packet to every candidate machine (which is the same way the *ping* tool works).
- Any addresses that respond are noted as active.

(1) **TCP Connect ( ) scan :** Another simple scan, an attacker attempts to open a standard TCP connection to a typical port on the candidate machine (such as the HTTP port 80). Any machine where such a connection succeeds is noted as active. Since many systems log any connection attempts, this type of scan is relatively easy to recognize from standard audit data.

(2) **UDP scans :** This scan consists of sending UDP packets to likely ports on candidate machines at worst, scanning for any open UDP ports. Since UDP is connectionless, such attempts are harder to control using filtering firewalls, and may be capable of finding unprotected services and hosts. Many variations on these scanning techniques exists – including scans using fragmented packets, and scans spread across a long period or a number of source machines. In practice, completely blocking scans is probably infeasible – but may give an administrator early warning of an impending attack.

(3) **Rlogin:** The RLOGIN attack is characterized by a high rate of connections from one node to another, often within a small period of time. In this attack, the intruder is attempting to gain access to the system.

Need of IDS

Intrusion Detection has its primary goal the detection of abuses of computer systems also it performs a variety of functions like :

- Monitoring and analyzing user and system activity.
- Auditing system configurations and vulnerabilities.
- Assessing the integrity of critical system and data files.
- Recognition of activity patterns reflecting known attacks.
- Statistical analysis for abnormal activity patterns.
- Operating-system audit-trail management, with recognition of user activity reflecting policy violations.
- IDS should offer reports of attacks in real time, ideally as the intrusion is in progress allowing security personnel to take corrective action.
- IDS should cooperate with other security mechanisms, increasing the overall security of systems. Ideally, IDS should be capable of detecting failures or attacks on other security mechanisms, forming a second level of defence.
- IDS should be capable of responding to intrusive behaviour: by increasing its monitoring in the relevant sections, or by excluding or restricting intrusive behaviour.
- IDS should protect itself against attacks, ensuring that the integrity of the greater system, and audit information up to the point of compromise remains intact, and ensuring that a compromised or hostile component cannot adversely affect the functioning of the system as a whole.

Other than monitoring network intruder and policy violations, the IDS can be useful in many other ways:

- To identify problem based on security policies.
- To maintain the logs of all the threat those are detected by IDS.
- As users are monitored continuously in network, making them analyze so that less violations cannot be committed.
- Using some preventive measures so that violation cannot be occur like terminating the network connections, user session or block access to the targets or the accounts that are likely to be violated.

- The IDPS (Intrusion Detection and Prevention System) can acts like proxy, which helps in un-packaging the payload of the request and remove header. This helps to invalidate the intruder attacks.
- The IDPS can sometimes change the security environment to prevent it from attacks.

5.5.1 Intrusion Detection Methods/ Techniques

→ (SPPU - Dec. 16)

Q. 5.5.5 Explain methods for intrusion detection system (IDS) (Ref. Sec. 5.5.1) Dec. 16, 6 Marks

The categorization of Detection methodologies are : Signature Based, anomaly based, stateful protocol analysis. Most of the IDPS uses these techniques to reduce or make network error free.

5.5.1(A) Signature Based Detection

- It is a process of comparing the signatures of known threat with the events that are been observed. Here the current packet is been matched with log entry of the signatures in the network.
- Signature is defined as the pattern (structure) that we search inside a data packet. The data packet may contain source address, destination address, protocol, port number etc.
- If an attacker adds any malicious code into these data packet he is generating attack pattern or signature.
- Signature based IDS create databases of such attack pattern for detecting the known or documented attacks. Single signature is used to detect one or more types of attacks which are present in different parts of a data packet.
- Signature based IDS used to monitor the events occurred in the network and match those events against a database of attack signatures to detect intrusions.
- It also uses a rule set to identify intrusions by watching for patterns of events specific to known and documented attacks.
- For example, we may get signatures in the IP header, transport layer header (TCP or UDP header) and application layer header or payload. Signature based intrusion detection system sometimes also called misuse detection techniques. It checks for the attack pattern with the existing stored database pattern and if match is found then generates the alert.
- Signature based IDSs are unable to detect unknown and newly generated attacks because it requires manual updating of each new type of attacks into to the existing database. The most well known example of signature - based IDS is SNORT IDS freely available for attack detection and study purpose.

Advantages

- An advantage of misuse-detection IDS is that it is not only useful to detect intrusions, but it will also detect intrusion attempts.
- Effective at detecting known attack without too many false alerts as compare to anomaly detection technique.
- Most of the current network intrusion detection system uses misuse detection technique for finding the attack pattern and detect them according to the rules and regulation used.
- Furthermore, the misuse detection IDS could detect port - scans and other events that possibly precede an intrusion.

Disadvantages

- Detecting only known attacks therefore it cannot identify new attacks efficiently.
- If there is single variation into attack signature it invalidates the attack signature or unable to detect it.
- Constant updating of attack pattern is required.

5.5.1(B) Anomaly Based Detection

→ (SPPU - May 16, May 17)

Q. 5.5.6 Explain Anomaly-based Instruction Detection System. (Ref. Sec. 5.5.1(B)) May 16, May 17, 6 Marks

- It is the process of comparing activities which are supposed to be normal against observed events to identify deviation.
- An IDPS uses Anomaly based detection techniques, which has profiles that represent normal activities of user, host, connections or applications.
- **For example :** Web activities are a normal activity done in a network. Anomaly based IDS works on the notation that "attack behavior" enough differ from "normal behavior" (IDS developer may define normal behavior).
- Normal or acceptable behaviours of the system (e.g. CPU usage, job execution time etc.) if the system behaviour looks abnormal i.e. increasing CPU speed, too many job execution at a time then it is assumed that the systems is out of normal activity. Anomaly based detection is based on the abnormal behaviour of a host or network.
- Database for such type of IDS is the events generated by user, host and network, and the "normal" behaviour of the systems. These events (historical data) are collected from the research laboratories which continuously work on normal and abnormal behaviour systems over a period of time.
- Anomaly based IDS checks ongoing traffic, host activities, transactions and behaviour in order to identify intrusions by detecting anomalies. Host - based IDS generally uses anomaly based techniques.
- This can be done in two ways:

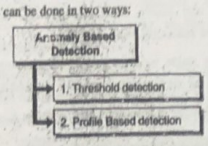

Fig. 5.5.2 : Anomaly based detection

➔ **1. Threshold detection**

Threshold is defined for all users for all groups and frequency of all events is measured comparing with threshold.

➔ **2. Profile Based detection**

Profiles of individuals are created and they are matched against the collected statistics for checking the irregular patterns.

☞ **Advantages**

An anomaly detection system observes and checks the deviation of normal network. If it observes any changes or suspicious in the network from normal deviations it will immediately inform and alert about the unknown attack.

☞ **Disadvantages**

- Anomaly detection techniques generate large number of false alarms due to the unpredictable behaviours of users and networks.
- It also requires extensive "training data set" of system events, records in order to characterize normal behaviour patterns.
- In addition, because a user's normal behaviour usually changes over time (for example, a user's behaviour may change when he moves from one host to another host), it is very difficult to collect the historical data of normal and abnormal behaviour.

5.5.1(C) Stateful Protocol Analysis

Unlike anomaly based detection which uses host and network specific profiles, the stateful protocol analysis relies on Vendor developed universal profiles. The stateful protocol analysis means the IDPS is able of checking the network, applications, and protocols that are pre defined in them. It can identify unexpected sequence of threats in form of commands.

☞ **Disadvantage of stateful protocol analysis**

- Stateful protocol analysis are extensively resource demanding.
- These methods don't capture threats or attacks that don't hamper the general accepted protocol in network.

Syllabus Topic : Types of IDs

5.5.2 Types of IDS

➔ **(SPPU - Dec. 16)**

Q. 5.5.7 Explain types of intrusion detection systems (IDS). (Ref. Sec. 5.5.2) **Dec. 16, 6 Marks**

Q. 5.5.8 Describe the different types of IDS and their limitations. (Ref. Sec. 5.5.2)

- The types of IDS are differentiated mainly by the types of event they monitor or scrutinize. There are four types of IDS.

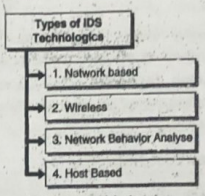

Fig. 5.5.3 : Types of IDS

➔ **1. Network based**

The IDS monitors network traffic. It analyzes the network activities and protocol activities to identify suspicious activity of the network.

➔ **2. Wireless**

The IDS monitors the wireless network traffic. It analyzes the network activities and protocol activities of wireless network.

➔ **3. Network Behaviour Analyse**

These network behavior analyze identify the treats that create unusual traffic overflow, DDOS (Distributed Denial of Service) attacks, malwares, and policy violations.

➔ **4. Host Based**

- These IDS monitors the host and the event occurs within that host.
- Among above four types of IDS two are important and most commonly used to monitor the networks and hosts.

5.5.2(A) Network based IDS (NIDS)

- As the usage and popularity of Internet is increasing tremendously, the attacks to the network are increasing for example TCP hijacking, DOS, IP Spoofing etc.

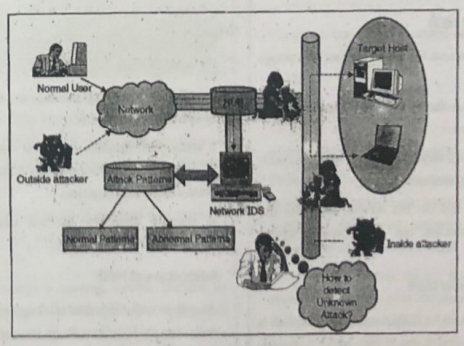

Fig. 5.5.4 : NIDS architect..re

- These network attacks cannot be detected by host based IDS It need Network based IDS to detect the attack and resolve it. General architecture of NIDS is shown in Fig. 5.5.4.
- NIDS detects attacks by monitoring, capturing and analyzing packets or network traffic and tries to give indication that computer has been misused. It detects malicious data present into packets by monitoring network traffic.
- NIDS continually monitors network traffic and discovers that if hacker/ intruder are attempting to break into a system.
- When NIDS installed on main server which consist of multiple hosts in a single network, it detects attacks present in the multiple hosts by checking incoming packets that looks unordinary.
- NIDS uses raw network packets as the training dataset for offline detection collected from well known research laboratory such as Defence Advance Research Project Agency (DARPA).
- As defined earlier it can be installed on servers, workstations, personal computers or machines dedicated to monitor incoming network packets from switches, routers and probes for intrusions.

Advantages of NIDS

- A well placed network - Based IDS can monitor a large network.
- NIDS just listen to the network; it does not interfere in the network.
- NIDS can be made very secure against attack and made invisible to many attackers.
- Network-based IDS use live network traffic for real time attack detection and also operating system independent.

Disadvantages of NIDS

- It becomes difficult for NIDS to recognize the attack in large or busy network due to high traffic is there in network. It will be difficult for NIDS to analyze.
- NIDS cannot analyze the network if communication is in encrypted format.
- Difficult to detect the whole process of attack, usually detect only the initial level of attack.
- We have seen a different type of IDS but we must know how these IDS detect whether given packet is malicious and the system behaviour is abnormal. There are two main types of detection techniques for analyzing events generation, system logs, audit trails, and malicious packet activities namely:anomaly detection and misuse detection also called signature based IDS.
- (NIDS) usually consists of a network sensor with a Network Interface Card (NIC) or LAN card operating in casual mode. The IDS is placed along a network segment or boundary and it monitors all traffic on that network segment.

5.5.2(B) Host Based IDS (HIDS)

HIDS usually collects information from the operating system audit trails, and system logs. (An audit trail is a series of records of computer events, about an operating system, an application, or user activities generated by an auditing system that monitors system activity). HIDS generally installed on individual host which is connected to the internet.

Features of HIDS

- HIDS focus monitoring and analyzing the computer system they are installed on.
- It continuously monitors the state of system. It check content of RAM and the file system to check that their content do not look suspicious.
- It generally looks for the real time malicious, suspicious activity of system log.

Advantages of HIDS

- As defined earlier Host-based IDS operate on OS audit trails; they can help detect Trojan horse or other attacks that creates the software integrity violation.

- HIDS analyze most of the encrypted network traffic, which usually encrypted or decrypted by the sender and/or receiver.
- It is able to monitor and detect attack, which is sometimes not possible for Network IDS.

Disadvantages of HIDS

- Host-based IDS are difficult to manage, because they generally installed on individual host. Monitoring to individual host is difficult because of different system configuration and log generation.
- When host-based IDS use operating system logs as an information source the amount of data can be increase, requiring additional local storage on the system.
- Host - based IDS are not suitable for detecting network denial of service and network scan attacks because it only checks only those packets received by individual host.

Syllabus Topic : Password Management, Limitations and Challenges

5.6 Password Management

→ **(SPPU - May 16, Dec. 16, May 17)**

Q. 5.6.1 List and explain any two password management practices. (Ref. Sec. 5.6) May 16, Dec. 16, May 17, 6 Marks

- In password management system the passwords can be created and stored very effectively. As many different users are using system all require their passwords for functioning in order to protect their data from each other.
- Another important aspect of password management is to disclose the passwords by a safe, secure and appropriate way.
- Password manager is important software available for password management. With the help of it passwords can be stored and organized. It stores passwords in an encrypted format.

Public Key Infrastructure

- Public Key Infrastructure (PKI) is a technology that uses mathematical algorithms and processes to facilitate secure transactions by providing data confidentiality, data integrity and authentication. PKI makes use of digital certificates to provide proof of identity for the individual.
- A digital certificate is a kind of digital document that binds a public key to a person for authentication, rather like a personal identity card. A trusted Certificate Authority (CA) creates the certificate and digitally signs it using the CA's private key, thereby authenticating the identity of the requestor.
- A person can use his or her certificate for authentication with different applications, and the applications then check the user's identity by verifying the digital signature with the issuing CA. PKI is particularly useful for user authentication in on-line transaction and public applications, because there is no advance pre-registration process required for each application. Users only need to apply for a certificate from a trusted CA to authenticate themselves with various applications.

Deploying PKI requires some worth noting security considerations as follows :

1. The private key must be protected and stored in a safe place, such as in a security token or smart card secured by a Pin.
2. Relevant password restrictions should be imposed on the PIN of the security token / smart card to prevent unauthorized access to the private key inside.
3. There should be proper procedures in place to handle key life-cycle management, issuing and revoking of certificates, storing and retrieving certificates and CRLs (Certificate Revocation Lists).
4. For private key backup, the key must be copied and stored in an encrypted form and protected at a level not lower than that of the original private key.
5. As not all applications support the use of PKI, there may be interoperability issues.

Single Sign-On

With the use of Single Sign-On (SSO) technology, users are able to identify themselves with the authentication server only once to access a variety of applications, including both internal and external systems. Users can enjoy the benefit of choosing one password to access multiple applications, instead of memorizing many different passwords

However, compromise of one authentication event could result in the compromise of all resources that the user has access rights to. Implementing SSO requires the following worth noting security considerations:

1. As one single authentication controls access to all resources, it is important that the authentication process is secure enough to protect those resources. This protection should satisfy the requirements of the most critical application. The single authentication process should not be weaker than the original authentication method used by the various applications, otherwise, the result is a downgrade in security level.
2. A second factor of authentication, such as a security token and smart card, can be used to strengthen the authentication process.
3. Relevant password restrictions, such as the minimum password length, the password complexity, the maximum number of trial attempts and the minimum time for renewal, and so on, should be imposed.
4. As the authentication server may become an attractive target for attack, it should be well protected so that intruders cannot access authentication information which could then be used for unauthorized access to all the systems.
5. Auditing and logging functions should be used to facilitate the detection and tracing of suspicious unsuccessful login attempts.
6. Encryption should be used to protect against authentication credentials transmitted across the network.

One-Time-Password Token

Another technology that may be used to facilitate password management is the one-time password token. Users authenticate themselves with two unique factors, something they have (the token) and something they know (the PIN).

Users do not need to choose or memorize passwords. The token will generate a unique, one-time-use password for each authentication process, based on the PIN and other factors, granting access to protected resources.

The following are some considerations when implementing one-time-password tokens :

1. A token is needed for each user of the authentication process, which implies additional investment.
2. Users must carry the token at all times, and they will not be able to access the system if they lose the token or forget to bring it with them. Unlike software based access control systems, which only require a password reset, users may not be able to use the system for hours or days if the token is lost.
3. Users should be aware of the physical security of the token and ensure that the token is properly protected at all times.
4. Most of the current one-time-password authentication schemes only authenticate the initial connection. Connections thereafter are assumed to be authenticated, and these connections are susceptible to being hijacked.
5. Security tokens may not support all applications or servers.

Best Practices

How to choose a good password of bad passwords? The following are examples of badly chosen passwords that can be easily guessed or cracked using password crackers freely available on the Internet.

- "password" - the most easily guessed password
- "administrator" - a login name
- "cisco" - a vendor"s name
- "peter chan" - a person"s name

- "aaaaaaaa" - repeating the same letter
- "abcdefgh" - consecutive letters
- "23456789" - consecutive numbers
- "qwertyui" - adjacent keys on the keyboard
- "computer" - a dictionary word
- "computer12" - simple variation of a dictionary word
- "c0mput3r" - simple variation of a dictionary word with "o" substituted by "0" and "e" substituted by "3"

To avoid falling prey to attackers, there are a number of simple rules that can be followed when creating a password : Password Management.

Don'ts

1. Do not use your login name in any form (as-is, reversed, capitalized, doubled, etc.).
2. Do not use your first, middle or last name in any form.
3. Do not use your spouse's or child's name.
4. Do not use other information easily obtained about you. This includes ID card numbers, license numbers, telephone numbers, birth dates, and the name of the street you live on, so on.
5. Do not use a password that contains all digits, or all the same letters.
6. Do not use consecutive letters or numbers like "abcdefgh" or "23456789".
7. Do not use adjacent keys on the keyboard like "qwertyui".
8. Do not use a word that can be found in an English or foreign language dictionary.
9. Do not use a word in reverse that can be found in an English or foreign language dictionary.
10. Do not use a well-known abbreviation e.g. HKSAR, HKMA, MTR.
11. Do not use a simple variation of anything described in 1-10 above. Simple variations include appending or prepending digits or symbols, or substituting characters, like 3 for E, $ for S, and 0 for O.
12. Do not reuse recently used passwords.
13. Do not use the same password for everything; have one password for non-critical activities and another for sensitive or critical activities.

Do's

1. Use a password with a mix of at least six mixed-case alphabetic characters, numerals and special characters.
2. Use a password that is difficult to guess but easy for you to remember, so you do not have to write it down.
3. Use a password that you can type quickly, without having to look at the keyboard, thereby preventing passers-by seeing what you are typing.

Things to note when handling passwords

(A) Don'ts

1. Do not write down your password, particularly anywhere near your computer or file it in a box file with the word "password" written on it.
2. Do not tell or give out your passwords to other people, even for a very good reason.
3. Do not display your password on the monitor.
4. Do not send your password unencrypted, especially via email.
5. Avoid using the "remember your password" feature associated with some websites, and disable this feature in your browser software.
6. Do not store your password on any media unless it is protected from unauthorized access (e.g. encrypted with an approved encryption method).

(B) Do's

1. Change your password frequently, at least every 90 days.
2. Change the default or initial password the first time you login.
3. Change your password immediately if you believe that it has been compromised. Once done, notify the system/security administrator for follow up action.

Syllabus Topic : Computer Intrusion

5.7 Computer Intrusion

- Unauthorized access to your computer/service/or data is called intrusion.
- Access could be physical or logical.
- Think of physical access as someone break-in to your house and access your computer using the username and password you have it on the posted notes next to the computer.
- Logical access is where attacker can access your computer/service or data over the network. He/she doesn't have to be physically on to your machine.
- Complete compromise is when you have root or administrator access to the computer, partial access is when you are able to log in as a user with limited rights or permission.

Chapter Ends...

□□□

Unit VI

CHAPTER 6

Confidentiality and Cyber Forensic

Syllabus

Introduction to Personally Identifiable Information (PII), Cyber Stalking, PII impact levels with examples Cyber Stalking, Cybercrime, PII Confidentiality Safeguards, Information Protection Law : Indian Perspective.

Syllabus Topic : Introduction to Personally Identifiable Information (PII)

6.1 Introduction to Personally Identifiable Information (PII)

Q. 6.1.1 Explain Personally Identifiable Information (PII). (Ref. Sec. 6.1)

- Personally Identifiable Information (PII) is any data that could potentially recognize a specific individual. Any information that can be used to tell apart one person from another and can be used for deanonymizing anonymous data can be considered PII.
- PII can be sensitive or non-sensitive. Non-sensitive PII is in order that can be transmitted in an unencrypted form without resulting in harm to the individual.
- Non-sensitive PII can be simply gathered from public records, phone books, corporate directories and websites.
- Sensitive PII is in turn which, when disclosed, could result in harm to the individual whose privacy has been breached.
- Sensitive PII should therefore be encrypted in transfer and when data is at rest. Such information adds biometric information, medical information, in Person Identifiable Financial Information (PIFI) and unique identifiers such as passport or Social Security numbers.

Syllabus Topic : Cyber Stalking

6.2 Cyber Stalking

Q. 6.2.1 What is Cyber stalking? Explain with example (Ref. Sec. 6.2)

- Cyber stalking is a crime in which the attacker harasses a victim using electronic message, such as e-mail or Instant Messaging (IM), or messages posted to a Web site or a discussion group.
- A cyber stalker relies upon the secrecy afforded by the Internet to allow them to stalk their victim without being detected.
- Cyber stalking messages differ from ordinary spam in that a cyber stalker targets a specific victim with often threatening messages, while the spammer targets a multitude of recipients with merely annoying messages.
- WHOA (Working to Halt Online Abuse), an online organization committed to the cyber stalking problem, reported that in 2001 58% of cyber stalkers were male and 32% female (presumably in some cases the perpetrator's gender is unknown). In a difference known as corporate cyber stalking, an organization stalks an individual.
- Corporate cyber stalking (which is not the same thing as corporate monitoring of e-mail) is usually initiated by a high-ranking company official with a grudge, but

may be conducted by any number of employees within the organization. Less frequently, corporate cyber stalking involves an individual pestering a corporation.

- WHOA reported that, in 2001, cyber stalking began with e-mail messages most frequently, followed by message boards and forums messages, and less frequently with chat. In some cases, cyber stalking develops from a real-world stalking incident and continues over the Internet.
- However, cyber stalking is also sometimes followed by stalking in the physical world, with all its assistant dangers. According to former U.S. Attorney General Janet Reno, cyber stalking is often "a prologue to more serious behaviour, including physical violence".
- In 1999, a New Hampshire woman was murdered by the cyber stalker who had endangered her in e-mail messages and posted on his Web site that he would kill her.
- There are a number of effortless ways to guard against cyber stalking. One of the most useful protection is to stay anonymous yourself, rather than having an identifiable online presence: Use your primary e-mail account only for communicating with people you trust and arrangement an anonymous e-mail account, such as Yahoo or Hotmail, to use for all your other communications.
- Set your e-mail program's filtering options to avert delivery of unwanted messages. When choosing an online name, make it different from your name and gender-neutral. Don't put any identifying particulars in online profiles.
- Should you become the victim of a cyber stalker? The most effective course of action is to report the criminal to their Internet service provider (ISP). Should that option be impossible, or unproductive? The best thing is to change your own ISP and all your online names.
- WHOA news that over 80% of cases reported in 2001 and 2002 were resolved by these methods, while 17% were reported to law enforcement officials.
- Cyber stalking, cyber squatting, and cyber terrorism are among the rising number of new computer and internet-related crimes, sometimes referred to collectively as cybercrime.

Syllabus Topic : PII Impact Levels with Examples Cyber Stalking

6.3 PII Impact Levels with Examples Cyber Stalking

Q. 6.3.1 Explain different impact levels of PII with an example. (Ref. Sec. 6.3)

Q. 6.3.2 Distinguish Cyber stalking from other acts. (Ref. Sec. 6.3)

- With the virtual world becoming part of the social lives of adults and minors alike, new attack vectors emerged to increase the severity of human-related attacks to a level the community have not experience before. This article finds out, shares and summarize on how technology could emerge further to counteract and mitigate the damage caused by online perpetrators.
- The review encourages approaching online harassment, nuisance, bullying, grooming and their likes with an Incident Response methodology in mind. This includes a detection phase utilizing automated methods to recognize and classify such attacks, conduct digital forensic investigations to analyse the nature of the offence and reserve evidence, taking preventive measures as part of the reaction towards the problem such as filtering unwanted communications and finally looking at how we can rely on applicable computing to support and educate thevictims.
- **Cyber stalking** is the use of the Internet or other electronic means to stalk or harass a person, group, or organization. It may include false accusations, defamation, slander and libel. It may also include monitoring, identity theft, threats, vandalism, solicitation for sex, or gathering information that may be used to threaten, embarrass or harass.
- Cyber stalking is often accompanied by real time or offline stalking. In many areas, such as California, both

are criminal offenses. Both are motivated by a desire to control, intimidate or influence a victim. A stalker may be an online stranger or a person whom the target knows. He may be anonymous and solicit involvement of other people online who do not even know the target.

- A stalker may be an online stranger or a person whom the person knows. He may be anonymous and solicit involvement of other people online who do not even know the target.
- Cyber stalking is a crime regarded in the US and many other judicial systems as more serious than a misdemeanourunder various state anti-stalking, slander and harassment laws.
- A conviction can result in a restraining order, probation, or criminal penalties against the attacker, including jail.
- There have been a number of attempts by experts and legislators to define cyber stalking. It is generally understood to be the use of the Internet or other electronic means to stalk or harass a person, a group, or an organization.
- Cyber stalking is a form of cyber bullying. The terms are frequently used interchangeably in the media. Both may include false accusations, defamation, slander and libel.
- Cyber stalking may also include monitoring, identity theft, threats, vandalism, solicitation for sex, or gathering information that may be used to threaten or harass.
- Cyber stalking is frequently accompanied by real-time or offline stalking. Both forms of stalking may be criminal offenses.
- Stalking is a continuous process, consisting of a series of actions, each of which may be entirely legal in itself.
- Technology ethics professor Lambèr Royakkers defines cyber stalking as perpetrated by someone without a current relationship with the victim. About the abusive effects of cyber stalking, he writes that, it is a form of mental assault, in which the perpetrator repeatedly, unwantedly, and disruptively breaks into the life-world of the victim, with whom he has no relationship (or no longer has), with motives that are directly or indirectly traceable to the affective sphere. Moreover, the separated acts that make up the intrusion cannot by themselves cause the mental abuse, but do taken together.

Distinguishing cyber stalking from other acts

- It is important to draw a distinction between cyber-trolling and cyber-stalking.
- Research has shown that actions that can be supposed to be harmless as a one-off can be considered to be trolling, whereas if it is part of a persistent campaign then it can be considered stalking.

Sr. No.	Motive	Mode	Gravity	Description
1	Playtime	Cyber-baatering	Cyber-trolling	In the moment and quickly regret
2	Tactical	Cyber-trickery	Cyber-trolling	In the moment but don't regret and continue
3	Strategic	Cyber-bullying	Cyber-stalking	Go out of way to cause problems, but without a sustained and planned long-term campaign
4	Domination	Cyber-hickery	Cyber-stalking	Goes out of the way to create rich media to target one or more specific individuals

- Cyber stalking author Alexis Moore separates cyber stalking from identity theft, which is economically motivated. Her definition, which was also used by the Republic of the Philippines in their legal description, is as follows : "Cyber stalking is a technologically-based

attack on one person who has been targeted particularly for that attack for reasons of anger, revenge or control".

- Cyber stalking can take many forms including :
  1. Harassment, embarrassment and humiliation of the victim
  2. Emptying bank accounts or other economic control such as defilement of the victim's credit score
  3. Harassing family, friends and employers to segregate the victim
  4. Scare tactics to instill fear and more.

Identification and detection

Q. 6.3.3 How one can identify and detect Cyber stalking? (Ref. Sec. 6.3)

Q. 6.3.4 List out the key factors in identifying Cyber stalking. (Ref. Sec. 6.3)

- Cyber Angels has written about how to identify cyber stalking :

  When identifying cyber stalking "in the field," and mostly when considering whether to report it to any kind of legal authority, the following features or combination of features can be considered to characterize a true stalking situation : malice, premeditation, repetition, distress, obsession, vendetta, no legitimate purpose, personally directed, disregarded warnings to stop, harassment and threats.

- A number of key factors have been identified in cyber stalking :
  - **False accusations :** Many cyber stalkers try to harm the reputation of their victim and turn other people against them. They post fake information about them on websites. They may set up their own websites, blogs or user pages for this purpose. They post allegations about the victim to newsgroups, chat rooms, or other sites that allow public contributions such as Wikipedia or Amazon.com.
  - **Attempts to gather information about the victim :** Cyber stalkers may advance to their victim's friends, family and work colleagues to obtain personal information. They may publicize information on the Internet, or hire a private detective.
  - Monitoring their target's online activities and attempting to trace their IP address in an attempt to gather more information about their victims.
  - **Encouraging others to annoy the victim :** Many cyber stalkers try to involve third parties in the annoyment. They may say the victim has harmed the stalker or his/her family in some way, or may post the victim's name and telephone number in order to encourage others to join the pursuit.
  - **False victimization :** The cyber stalker will claim that the victim is annoying him or her. Bocij writes that this fact has been noted in a number of well-known cases.
  - **Attacks on data and equipment :** They may try to harm the victim's computer by sending viruses.
  - **Ordering goods and services :** They order items or subscribe to magazines in the victim's name.
- These frequently involve subscriptions to pornography or ordering sex toys then having them delivered to the victim's workplace.
- **Arranging to meet :** Young people face a particularly high risk of having cyber stalkers try to set up meetings between them.
- The posting of defamatory or derogatory statements: Using web pages and message boards to incite some response or reaction from their victim.

Prevalence and impact

Q. 6.3.5 Write a short note on : Prevalence and impact. (Ref. Sec. 6.3)

- According to Law Enforcement Technology, cyber stalking has increased exponentially with the expansion of new technology and new ways to stalk victims.

- Disgruntled employees pose as their bosses to post open messages on social network sites, spouses use GPS to track their mates' every move.
- Even police and prosecutors find themselves at risk, as gang members and other organized criminals come across where they live - frequently to intimidate them into dropping a case.
- In January 2009, the Bureau of Justice Statistics in the United States released the study "Stalking Victimization in the United States", which was sponsored by the Office on Violence Against Women.
- The report, based on supplemental data from the National Crime Victimization Survey, showed that one in four stalking sufferers had been cyber stalked as well, with the perpetrators using internet-based services such as email, instant messaging, GPS, or spyware.
- The final report stated that around 1.2 million victims had stalkers who used technology to find them.
- The Rape, Abuse and Incest National Network (RAINN), in Washington D.C. has released statistics that there are 3.4 million stalking sufferer each year in the United States. Of those, one in four reported experiencing cyber stalking.
- According to Robin M. Kowalski, a social psychologist at Clemson University, cyber bullying has been shown to cause higher levels of anxiety and depression for sufferer than normal bullying.
- Kowalksi states that much of this stems from the anonymity of the perpetrators, which is a common feature of cyber stalking as well. According to a study by Kowalksi, of 3,700 bullied middle-school students, a quarter had been subjected to a form of annoyment online.

Types

Q. 6.3.6 Enlist the different types of Cyber stalker attacks. (Ref. Sec. 6.3)

1. **Stalking by strangers**
   - According to Joey Rushing, a District Attorney of Franklin County, Alabama, there isn't a lone definition of a cyber stalker - they can be either strangers to the prey or have a former/present relationship.
   - "Cyber stalkers come in all shapes, sizes, ages and backgrounds. They tour Web sites looking for an opportunity to take advantage of people".
2. **Gender-based stalking**
   - Annoyment and stalking because of gender online is common, and can include rape threats and other threats of violence, as well as the posting of the sufferer's personal information.
   - It is blamed for limiting sufferer activities online or driving them offline entirely, thereby impeding their participation in online life and undermining their autonomy, dignity, identity, and opportunities.
3. **Of intimate partners**
   - Cyber stalking of intimate partners is the online annoyment of a current or former romantic partner. It is a form of domestic violence, and experts say its purpose is to control the victim in order to encourage social isolation and create dependency.
   - Annoyers may send repeated insulting or threatening e-mails to their sufferer, monitor or disrupt their sufferer' e-mail use, and use the victim's account to send e-mails to others posing as the victim or to purchase goods or services the victim does not want. They may also use the Internet to research and compile personal information about the victim, to use in order to annoy him or her.
4. **Of celebrities and public persons**
   - Profiling of stalkers shows that about always they stalk someone they know or, via delusion, think they know, as is the case with stalkers of celebrities or public persons in which the stalkers feel they know the celebrity yet the celebrity does not know them. As part of the risk they take for being in the public eye,

celebrities and public figures are frequently targets of lies or made-up stories in tabloids as well as by stalkers, some even seeming to be fans.

- In one noted case in 2011, actress Patricia Arquette quit Facebook after suspected cyber stalking. In her last post, Arquette explained that her security warned her Facebook friends to never accept friend requests from people they do not really know.
- Arquette stressed that just because people seemed to be fans did not mean they were safe. The media issued a statement that Arquette planned to communicate with fans entirely through her Twitter account in the future.

5. By anonymous online mobs

- Web 2.0 technologies have enabled online groups of anonymous people to self-organize to target individuals with online defamation, fear of violence and technology-based attacks.
- These include publishing lies and doctored photographs, threats of rape and other violence, posting sensitive personal information about sufferer, e-mailing damaging statements about sufferer to their employers, and manipulating search engines to make damaging material about the victim more prominent.Sufferer frequently respond by adopting pseudonyms or going offline entirely.
- Experts attribute the destructive nature of anonymous online mobs to group dynamics, saying that groups with homogeneous views tend to become more extreme.
- As members reinforce each others' beliefs, they fail to see themselves as individuals and lose a sense of personal responsibility for their destructive acts. In doing so they dehumanize their sufferer, becoming more aggressive when they believe they are supported by authority figures. Internet service providers and website owners are sometimes blamed for not speaking out against this type of annoyment.
- A notable example of online mob annoyment was the experience of American software developer and blogger Kathy Sierra.
- In 2007 a group of anonymous individuals attacked Sierra, threatening her with rape and strangulation, publishing her home address and Social Security number, and posting doctored photographs of her. Frightened, Sierra cancelled her speaking engagements and shut down her blog, writing "I will never feel the same. I will never be the same".

6. Corporate cyberstalking

- Corporate cyberstalking is when a company annoyes an individual online, or an individual or group of individuals annoyes an organization.
- Motives for corporate cyberstalking are ideological. or include a desire for financial gain or revenge.

Perpetrators

Q. 6.3.7 What is mean by Perpetrators? (Ref. Sec. 6.3)

Motives and profile

- Mental profiling of digital criminals has identified psychological and social factors that motivate stalkers as: envy; pathological fascination (professional or sexual); unemployment or failure with own job or life; intention to threaten and cause others to feel inferior; the stalker is delusional and believes he/she "knows" the target; the stalker wants to in still fear in a person to justify his/her status; belief they can get away with it(anonymity); threats for financial advantage or business competition; revenge over perceived or imagined rejection.

Four types of cyber stalkers

- Preliminary work by Leroy McFarlane and Paul Bocij has identified four types of cyber stalkers. The vindictive cyber stalkers noted for the ferociousness of their attacks. The composed cyber stalker whose motive is to annoy. The fiendish cyber stalker who attempts to form a relationship with the victim but turns on them if rebuffed and collective cyber stalkers, groups with a motive.

- According to Antonio Chacón Medina, author of Unaonevacara de Internet, El acoso ("A new face of the Internet: stalking"), the general profile of the annoyer is cold, with little or no respect for others.
- The stalker is a predator who can wait patiently until vulnerable sufferer appear, such as women or children, or may enjoy pursuing a particular person, whether personally familiar to them or unknown.
- The annoyer enjoys and demonstrates their power to pursue and psychologically damage the victim.

Behaviours

- Cyber stalkers find their sufferer by using search engines, online forums, bulletin and discussion boards, chat rooms, and more recently, through social networking sites, such as MySpace, Facebook, Bebo, Friendster, Twitter, and Indymedia, a media outlet known for self-publishing. They may engage in live chat annoyment or flaming or they may send electronic viruses and unsolicited e-mails.
- Cyberstalkers may research individuals to feed their obsessions and curiosity. Conversely, the acts of cyberstalkers may become more strong, such as repeatedly instant messaging their targets.
- More commonly they will post defamatory or offensive statements about their stalking target on web pages, message boards, and in guest books designed to get a reaction or response from their victim, thereby initiating contact.
- In some cases, they have been known to generate fake blogs in the name of the victim containing defamatory or pornographic content.
- When prosecuted, many stalkers have unsuccessfully attempted to validate their behavior based on their use of public forums, as opposed to direct contact.
- Once they get a reaction from the victim, they will usually attempt to track or follow the victim's internet activity.
- Classic cyber stalking behavior includes the tracing of the sufferer's IP address in an attempt to verify their home or place of employment.
- Some cyber stalking situations do develop into physical stalking, and a victim may experience abusive and excessive phone calls, vandalism, threatening or obscene mail, trespassing, and physical assault.
- Moreover, many physical stalkers will use cyberstalking as another method of annoying their sufferer.
- A 2007 study led by Paige Padgett from the University of Texas Health Science Center initiate that there was a false degree of safety assumed by women looking for love online.

Syllabus Topic : Cybercrime

6.4 Cybercrime

Q. 6.4.1 Define Cybercrime and discuss its types. (Ref. Sec. 6.4)

- The crime that involves and uses computer devices and Internet is known as cybercrime.
- Cybercrime can be committed in opposition to an individual or a group; it can also be committed against government and private organizations. It may be planned to harm someone's reputation, physical harm, or even mental harm.
- Cybercrime can cause direct harm or indirect harm to whoever the sufferer is.
- However, the largest threat of cybercrime is on the financial security of an person as well as the government.
- Cybercrime causes loss in billions each year.

Types of Cybercrime

Let us now discuss the most important types of cybercrime.

1. **Hacking**

- It is an unlawful practice by which a hacker breaches the computer's security system of someone for personal interest.

2. **Unwarranted mass-surveillance**

- Mass surveillance means surveillance of a considerable fraction of a group of people by the authority especially for the security purpose, but if someone does it for personal interest, it is considered as cybercrime.

3. **Child pornography**

- It is one of the most atrocious crimes that is brazenly practiced across the world.
- Children are sexually abused and videos are being made and uploaded on the Internet.

4. **Child grooming**

- It is the practice of establishing an emotional connection with a child mainly for the purpose of child-trafficking and child prostitution.

5. **Copyright Infringement**

- If someone infringes someone's protected exclusive rights without permission and publishes that with his own name, is known as copyright infringement.

6. **Money laundering**

- Unlawful possession of money by an individual or an organization is known as money laundering. It typically involves transfers of money through foreign banks and/or legal business.
- In added words, it is the practice of transforming illegitimately earned money into the legitimate financial system.

7. **Cyber-extortion**

- When a hacker hacks someone's email server, or computer system and load money to reinstate the system, it is known as cyber-extortion.

8. **Cyber-terrorism**

- Normally, when someone hacks government's security system or intimidates government or such a big organization to move forward his political or social objectives by invading the security system through computer networks, it is known as cyber-terrorism.

Syllabus Topic : PII Confidentiality Safeguards

6.5 PII Confidentiality Safeguards

Q. 6.5.1 Discuss PII confidentiality safeguards. (Ref. Sec. 6.5)

- Personally identifiable information (PII) is any information that can be used to recognize, contact, or locate an individual, either alone or combined with other easily accessible sources.
- It includes information that is connected or linkable to an individual, such as medical, educational, financial and employment information.
- Examples of data elements that can identify an individual contain name, fingerprints or other biometric (including genetic) data, email address, telephone number or social security number.
- Safeguarding university-held PII (and other sensitive information) is the accountability of each and every member of the University's workforce. Regardless of your role, you should know what PII is and your accountability in ensuring its protection.
- Although society has always relied on personal identifiers, essential and protecting PII has recently become much more important as a component of personal privacy, now that advances in computing and communications technology, including the internet, has made it easier to collect and process vast amounts of information.
- The protection of PII and the on the whole privacy of information are concerns both for individuals whose personal information is at stake and for organizations that may be liable or have their reputations spoiled

should such PII be inappropriately accessed, used, or disclosed. Examples of laws related to different types of PII are listed below :

- HIPAA/HITECH - Health related information.
- GLBA - Financial information.
- Privacy Act - Fair Information Practices for PII held by Federal Agencies.
- COPPA - Protects children's privacy by allowing parents to control what information is collected.
- FERPA - Student's personal information.
- FCRA - Collection and use of consumer information.

- Such laws attempt to restrict corporations from incorrectly sharing PII and impose requirements for appropriately protecting such information.
- Legally collecting and selling PII has become lucrative, but PII can also be exploited by criminals to steal a person's identity or commit other crimes.
- According to FBI statistics, identity theft continues to be one of the nation's fastest growing crimes and can cause both financial and emotional damage to its sufferer. Due to this threat, many governments have enacted legislation to bound the distribution of personal information.
- The following list contains examples of information that may be considered PII.
  - Name, such as full name, maiden name, mother's maiden name, or alias
  - Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, and financial account or credit card number
  - Address information, such as street address or email address
  - Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people
  - Telephone numbers, including mobile, business, and personal numbers
  - Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry)
  - Information identifying personally owned property, such as vehicle registration number or title number and related information
  - Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information)

Syllabus Topic : Information Protection Law - Indian Perspective

6.6 Information Protection Law : Indian Perspective

Q. 6.6.1 Explain information protection law : Indian perspective. (Ref. Sec. 6.6)

Q. 6.6.2 What are different types of attacks by Hackers? (Ref. Sec. 6.6)

Q. 6.6.3 Explain the terms :
(i) Virus (ii) Phishing
(iii) Spoofing (iv) Phone phishing
(v) Internet phaming (Ref. Sec. 6.6)

What Is Cyber Crime?

- Cyber terrorists typically use the computer as a tool, target, or both for their unlawful act either to gain information which can result in heavy loss/damage to the owner of that intangible sensitive information.
- Internet is one of the way by which the offenders can gain such price sensitive information of companies,

firms, individuals, banks, intellectual property crimes (such as stealing new product plans, its description, market programme plans, list of customers etc.), selling unlawful articles, pornography etc.

- This is done through many methods such as phishing, spoofing, pharming, internet phishing, wire transfer etc. and use it to their own advantage without the permission of the individual.
- Many banks, financial institutions, investment houses, brokering firms etc. are being victimized and endangered by the cyber terrorists to pay extortion money to keep their sensitive information intact to avoid huge damages.
- And its been reported that many institutions in US, Britain and Europe have furtively paid them to prevent huge meltdown or collapse of confidence among their consumers.

Emergence of Information Technology Act, 2000

- In India, the Information Technology Act 2000 was enacted after the United Nation General Assembly Resolution A/RES/51/162, dated the 30th January, 1997 by adopting the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law.
- This was the first step towards the Law involving to e-commerce at international level to regulate an alternative form of commerce and to give legal status in the area of e-commerce. It was enacted taking into thought UNICITRAL model of Law on e-commerce 1996.
- Some notable Provisions Under The Information Technology Act, 2000.
  - Sec. 43 : Damage to Computer system etc.
  - Sec. 66 : Hacking (with objective or knowledge) Compensation for Rupees 1crore. Fine of 2 lakh rupees, and captivity for 3 years.
  - Sec. 67 : Publication of obscene material in e-form Fine of 1 lakh rupees, and captivity of 5years, and double conviction on ... d offence.
  - Sec. 68 : Not com... g with directions of controller
  - Sec. 70 : Attempting ... securing access to computer.
  - Sec. 72 : For breaking confidentiality of the information of compu...
  - Sec. 73 : Publishing false digital signatures, false in certain particulars
  - Sec. 74 : Publication of Digital Signatures for fraudulent purpose Fine upto 2 lakh and imprisonment of 3 years.
- Captivity upto 10 years. Fine upto 1 lakh and imprisonment upto 2 years Fine of 1 lakh, or imprisonment of 2 years or bo... Captivity for the term of 2 years and fine for 1 lakh r... es.

Types of Attacks By Hac...

- Hacker is computer expert who uses his knowledge to get unauthorized access to the c...puter network. He is not any person who intends to br...k through the system but also includes one who has no intention todamage the syste... but intends to lea... more by using ones computer.
- Crackers on other hand use the information cause disruption to the network for personal and political motives. Hacking by an insider ... an employee is pretty prominent in present da... tion 66(b) of the Information Technology ... 2000, provides punishment of imprisonment for the period of 3 years and fine which may extent to two lakhs rupees,or with both.
- Banks and other financial insti... tions are threatened by the terrorist groups to use ... sensitive information resulting in deep loss and ... ask for ransom amount from them. There are ... methods used by hackers to gain unauthorised ... ss to the computers distant from use of viruses like Trojans and worms etc.

- Therefore if anyone secures access to any computer without the permission of the owner shall be likely to pay damages of 1 crore rupees under Information Technology Act, 2000.
- Computer system here means a device including input and output support devices and systems which are capable of performing logical, arithmetical, data storage and reclamation, communication control and other functions but excludes calculators.
- Unauthorised access under Section 43 of the Information Technology Act 2000 is punishable regardless of the intention or purpose for which unauthorised access to the computer system was made. Owner needn't prove the facto of loss, but the fact of it been used without his authorisation.
- Case of **United States v. Rice** would be important in this consider where defendant on the request of his friend (who was been beneath investigation by IRS officer) tried to find the status of his friends case by using officers computer without his approval.
- Though it didn't cause any spoil/loss to the plaintiff (officer) but was convicted by the Jury for accessing the computer system of a Government without his authority and his sincerity was later on confirmed. Even if one provides any help to the other to gain any unauthorised access to the computer he shall be liable to pay damages by way of compensation of Rupees 1 crore.
- Does turning on the computer leads to unauthorized access? The mensrea under section 1 of the Computer misuse Act, 1990 comprises of two elements there must be an intent to secure an access to any programme or data held in any computer, and the person must know that he intends to secure an unauthorized access.
- Though section 1 (1) (a) requires that second computer must be involved but the judiciary in the case of R v. Sean Cropp, believed that the Parliament would have intended to limit the offence even if single computer system was involved.

(A) Computer Viruses

- Viruses are used by Hackers to contaminate the user's computer and dent data saved on the computer by use of payload in viruses which carries damaging code.
- Person would be liable under I.T Act only when the consent of the owner is not taken before inserting virus in his system.
- The contradiction here is that though definite viruses causes temporary interruption by showing messages on the screen of the user but still its not punishable under Information Technology Act 2000 as it doesn't cause tangible damage.
- But, it must be made punishable as it would plunge under the ambit of unauthorised access though doesn't cause any damage.
- Harmless viruses would also plunge under the expression used in the provision to unsurp the normal operation of the computer, system or network. This ambiguity needs reconsideration.

(B) Phishing

- By using e-mail messages which entirely resembles the original mail messages of customers, hackers can as... for verification of certain information, like account numbers or passwords etc.
- Here customer might not have knowledge that the e-mail messages are unreliable and would fail to identify the originality of the messages.This results in huge financial loss when the hackers use that information for fraudulent acts like withdrawing money from customers account without him having knowledge of it.

(C) Spoofing

- This is carried on by use of unreliable Websites or e-mails.
- These sources copy the original websites so well by use of logos, names, graphics and even the code of real banks site.

(D) Phone Phishing

- Is done by use of in-voice messages by the hackers where the customers are asked to disclose their account identification, and passwords to file a complaint for any problems regarding their accounts with banks etc.

(E) Internet Pharming

- Hacker here aims at redirecting the website used by the customer to another fake website by hijacking the sufferer DNS server (they are computers responsible for resolving internet names into real addresses - signposts of internet), and changing his IP address to fake website by manipulating DNS server. This redirects user's original website to a false deceptive website to gain unauthorised information.

(F) Risk Posed On Banks and Other Institutions

- Wire transfer is the means of transferring money from one account another or transferring cash at cash office. This is most convenient way of transfer of cash by customers and money laundering by cyber terrorists.
- There are many guidelines issued by Reserve Bank of India (RBI) in this view, one of which is KYC (Know Your Customer) norms of 2002. Main objective of which is to :
  1) Ensure appropriate customer identification, and
  2) Monitor the transaction of suspicious nature and report it to appropriate authority every day bases.

(G) Publishing Pornographic Material In Electronic Form

- Section 67 of the Information Technology Act, 2000 in parallel to Section 292 of Indian Penal Code, 1860 makes publication and broadcast of any material in electronic that lascivious or appeals to the prurient interest a crime, and punishable with captivity which may extend to 5 years and fine of 1 lakh rupees and subsequent offence with an captivity extending to 10 years and fine of 2 lakhs.
- Various tests were laid down slowly in course of time to determine the actual crime in case of obscene material published in electronic form on net.
- Hicklin test was adopted in America in the case of Regina v. Hicklin wherein it was seized that if the material has tendency is to deprive and corrupt those whose minds are open to such immoral influences, and into whose hands a publication of this sort may fall.
- In Indian situation the case of Ranjeet D. Udeshi v. State of Maharashtra the Supreme Court admitted that Indian Penal Code doesn't term obscenity though it provides punishment for publication of obscene matter.
- There are very thin line existing between a material which could be called obscene and the one which is artistic.
- Court even strained on need to maintain balance between fundamental right of freedom of speech and expression and public decency and morality. If matter is likely to degrade and corrupt those minds which are open to influence to whim the material is likely to fail. Where both obscenity and artistic matter is so mixed up that obscenity fails into shadow as its insignificant then obscenity may be overlooked.
- In the case of Miller v. California it was held that local community standard must be applied at the time of determination of the offence.
- As it can traverse in many jurisdictions and can be accessed in any part of the globe. So wherever the material can be accessed the community standards of that country would be applicable to determine the offence of publication of obscene material posted in electronic form. Though knowledge of obscenity under Information Technology Act 2000 and Indian Penal Code may be taken as justifying factor but doesn't take the case out of the provision.
- Section 72 of Information Technology Act, 2000 provides punishment for an unauthorised access or, exposé of that information to third person punishable with an captivity upto 2 years or fine which may extend to 1 lakh rupees or with both.

- English courts have also dealt with an issue as to what activities would form crime under existing legislation, in the case of R. v. Fellows and Arnold it was held that the legislation before the 1994 amendment would also facilitate computer data to be considered a copy of an indecent photograph and making images available for downloading from the website would constitute material being distributed or shown.
- Statute is wide enough to deal with the use of computer technology.

(H) Investment Newsletter

- We usually get newsletter providing us free information recommending that investment in which field would be lucrative.
- These may sometimes be a fraud and may origin us huge loss if relied upon.
- False information can be spread by this method about any company and can cause massive inconvenience or loss through junk mails online.

(I) Credit Card Fraud

- Huge loss may reason to the victim due to this kind of fraud. This is done by publishing false digital signatures.
- Most of the people misplace credit cards on the way of delivery to the recipient or its damaged or defective, misrepresented etc.

Measures to Curb the Crime

- Though by course of time and improvement in technology to provide easier and user friendly methods to the consumer for make up their daily activities, it has lead to harsh world of security threats at the same time by agencies like hackers, crackers etc.
- Various Information technology methods have been introduced to curb such destructive activities to achieve the main objects of the technology to provide some sense of security to the users.

Few basic major measures used to curb cyber crimes are as follows :

(A) Encryption

- This is considered as an important tool for shielding data in transit. Plain text (readable) can be converted to cipher text (coded language) by this method and the recipient of the data can decrypt it by converting it into plain text again by using private key. This way excluding for the recipient whose possessor of private key to decrypt the data, no one can gain access to the sensitive information.
- Not only the information in transit but also the information stored on computer can be protected by using Conventional cryptography method.
- Usual problem lies during the allocation of keys as anyone if overhears it or intercept it can make the whole object of encryption to standstill.
- Public key encryptography was one solution to this where the public key could be known to the whole world but the private key was only identified to receiver. It's very difficult to derive private key from public key.

(B) Synchronized Passwords

- These passwords are schemes used to change the password at users and host token. The password on synchronized card changes every 30-60 seconds which only makes it legitimate for one time log-on session.
- Other functional methods introduced are signature, voice, fingerprint identification or retinal and biometric recognition etc. to impute passwords and pass phrases.

(C) Firewalls

- It creates wall between the system and possible intruders to protect the confidential documents from being leaked or accessed.
- It would only let the data to flow in computer which is known and verified by ones system. It only permits access to the system to ones already registered with the computer.

(D) Digital Signature

- Are created by using means of cryptography by applying algorithms.
- This has its important use in the business of banking where customers signature is identified by using this method before banks enter into huge transactions.

Investigations and Search Procedures

- Section 75 of Information Technology Act, 2000 takes care of jurisdictional part of cyber crimes, and one would be punished irrespective of his nationality and place of commission of offence.
- Power of inquiry is been given to police officer not below the rank of Deputy Superintendent of police or any officer of the Central Government or a State Government authorised by Central Government.
- He may enter any public place, conduct a search and arrest without warrant person who is reasonably expected to have committed an offence or about to commit computer related crime.
- Accused has to be shaped before magistrate within 24 hours of arrest. Provisions of Criminal Procedure Code, 1973 regulate the procedure of entry, search and arrest of the accused.

6.7 Problems Underlying Tracking of Offence

Q. 6.7.1 What are the challenges the system face to track the offence ? (Ref. Sec. 6.7)

- Most of the times the offenders commend crime and their identity is hard to be identified. Tracking cyber criminals requires a proper law enforcing agency through cyber border co-operation of governments, businesses and institutions of additional countries.
- Most of the countries not have skilled law enforcement personnel to deal with computer and even broader Information technology related crimes.
- Usually law enforcement agencies also don't take crimes serious, they have no significance of enforcement of cyber crimes, and even if they undertake to investigate they are posed with limitation of extra-territorial nature of crimes.

How Efficient Is Information Technology Act 2000 ?

- It can't be disputed that Information Technology Act, 2000 though provides definite kinds of protections but doesn't cover all the spheres of the I.T where the protection must be provided.
- Copyright and trade mark violations do occur on the net but Copy Right Act 1976, or Trade Mark Act 1994 are quiet on that which specifically deals with the issue. Therefore have no enforcement machinery to ensure the protection of domain names on net.
- Transmission of e-cash and transactions online are not given protection under Negotiable Instrument Act, 1881. Online privacy is not protected only Section 43 (penalty for damage to computer or computer system) and 72 (Breach of confidentiality or privacy) talks about it in some extent but doesn't hinder the violations caused in the cyberspace.
- Even the Internet Service Providers (ISP) who provides some third party information without human intervention is not made liable under the Information Technology Act, 2000.
- One can easily take cover under the exemption clause, if he proves that it was committed without his knowledge or he exercised due diligence to avert the offence. Its hard to prove the commission of offence as the terms due diligence and lack of knowledge have not been clear anywhere in the Act.
- And unfortunately the Act doesn't mention how the extra territoriality would be imposed. This aspect is completely ignored by the Act, where it had come into existence to look into cyber crime which is on the face of it an international problem with no territorial boundaries.

Data Protection

- Information stored on the owner of the computer would be his property and must be protected there are many ways such information can be misrepresented by ways like unauthorized access, computer viruses, data typing, modification erasures etc.
- Legislators had been continuously confronted with problem in balancing the right of the individuals on the computer information and other peoples claim to be allowed access to information under Human Rights.
- The first enactment in this regard was Data Protection Act by Germany in the year 1970. This was widely received by the world and also contributed to the Information Technology Act.
- The origin of laws on date protection dates back to 1972 when United Kingdom created a committee on privacy which came up with ten principles, on the bases of which data protection committee was set up.
- Data Protection Act, 1984 (DPA) was United Kingdoms response to the Council of Europe Convention 1981, this Act lacked proper enforcement mechanism and has done little to enforce individuals rights and freedoms.
- European Union directive in 1995, European Convention of Human Rights (ECHR), Human Rights Acts, and further introduction of Data Protection Act, 1998 have done a large amount in the field of Data protection in today's date.
- Date Protection Act has following aims and objectives: Personal information shall only be obtained for lawful purpose, it shall only be used for that purpose, mustnot be disclosed or used to effectuate any unlawful activity, and must be disposed off when the purpose is satisfied.
- Though Data Protection Act aims at protecting privacy issues related to the information but still we find no reveal of the word privacy in the Act, nor is it defined, further the protection comes with various exemptions, including compulsory notification from the Commissioner in certain cases of the personal data.
- Due to the change in the regime of information technology for the date European Convention came, on which the Act is based changes in the Act is advised for matching the present situation and curbing the crime in efficient way.
- There is no Data Protection Act in India, the only provisions which talks about data protection are Section 72 and Section 43 of Information Technology Act, 2000.
- There must be a new Law to deal with the situation for a person to know that the checker is processing his data concerning him and also that he must know the purpose for which it has been processed.
- It is a fundamental right of the Individual to hold private information concerning him provided under Article 21 of the Indian Constitution, which says: No person shall be rundown of his life or personal liberty except according to procedure established by law.
- And due to the increasing trend of the Crime rate in the field separate legislation is required in this environment for better protection of individuals.

Chapter Ends...

□□□